

SELECT COMMITTEE ON
SCIENCE AND TECHNOLOGY

**DIGITAL IMAGES
AS EVIDENCE**

EVIDENCE

Ordered to be printed 3 February 1998

LONDON: THE STATIONERY OFFICE

£17.80

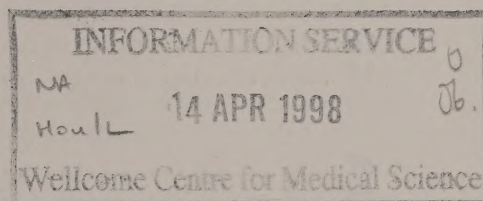


22501831088

SELECT COMMITTEE ON
SCIENCE AND TECHNOLOGY

**DIGITAL IMAGES
AS EVIDENCE**

EVIDENCE



Digital television 12457
Evidence (Law)

Ordered to be printed 3 February 1998

LONDON: THE STATIONERY OFFICE

£17.80

CONTENTS

	<i>Page</i>
CALL FOR EVIDENCE	v
ORAL EVIDENCE	
<i>Justice and Liberty</i>	
Written evidence	1
Oral evidence, 23 October 1997	19
<i>Mr Simon Davies, Privacy International</i>	
Written evidence	31
Oral evidence, 23 October 1997	32
<i>Mr Graham Smith, Bird & Bird and Mr Harry Small, Baker & McKenzie</i>	
Oral evidence, 6 November 1997	36
<i>Mr Peter Sommer, London School of Economics</i>	
Written evidence	43
Oral evidence, 6 November 1997	48
<i>Local Government Information Unit</i>	
Written evidence	55
Oral evidence, 20 November 1997	59
<i>British Standards Institution</i>	
Written evidence	67
Oral evidence, 20 November 1997	71
<i>Data Protection Registrar</i>	
Written evidence	76
Oral evidence, 27 November 1997	85
<i>IBM United Kingdom Ltd</i>	
Written evidence	95
Oral evidence, 4 December 1997	102
<i>Abbey National plc</i>	
Written evidence	109
Oral evidence, 4 December 1997	109
<i>Essex Police Constabulary</i>	
Written evidence	115
Oral evidence, 11 December 1997	117
<i>Home Office and the Forensic Science Service</i>	
Written evidence	124
Oral evidence, 11 December 1997	137
WRITTEN EVIDENCE	
Security Facilities Executive (SAFE)	145
Mr Grady Miller, Trade Policy Analyst	146
Press complaints Commission	149
Symonds Group Ltd	150
Broadcasting Standards Commission	151
Association of Chief Police Officers in Scotland	153
Law Society of Scotland	155

	Page
Chartered Institute of Arbitrators (Scottish Branch)	156
Screen plc	157
AEA Technology	158
Dr Stephen Castell, Computer and Systems Telecommunications Ltd	159
The Lord Brain	160
The Faculty of Advocates	166
Crown Prosecution Service	167
Professor Vicki Bruce, University of Stirling	169
Niels J Bjergstrom, Information Security Bulletin	170
Office of Public Service Central IT Unit	171
Dr Nigel D Haig	171
General Council of the Bar	172

CALL FOR EVIDENCE

The House of Lords Science and Technology Committee has appointed Sub-Committee II, under the chairmanship of Lord Craig of Radley, to conduct an enquiry into the use of digital images as evidence.

Because digital images are easy to copy and it may be difficult to distinguish a copy, or a copy which has been "doctored", from the original, concern has been raised over their use as evidence. As analogue systems are being displaced by digital ones and the investment in digital technology for image capture and signal processing increases, it is important that any concerns over the use of this technology be addressed now if wise investment decisions are to be made.

The enquiry will examine the need for any special measures to ensure the integrity and authenticity of digital images. It will consider if any measures are necessary to ensure that modern image processing technologies, such as compression and enhancement techniques when applied to either digital or analogue images, are acceptable in court. It will also examine the implications of video surveillance technologies for civil liberties.

The Sub-Committee invites written submissions on all matters relevant to this topic, but in particular on the questions listed below, with a view to making a report to the House of Lords early in 1998.

1. What is the current and forecast future use of digital technology for image collection, storage and transmission? What is its use by the courts and the legal profession? What is the state of the art of image manipulation?
2. Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean they should be treated differently when used as evidence?
3. Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence? What would be the preferred practical measure?
4. Under what circumstances and with what controls should modified or enhanced images be used as evidence?
5. Do technologies which compress data or use error correction technology when transmitting it raise special problems?
6. Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?
7. Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?
8. Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?
9. Is there the need for special measures to control the publication of modified images by the media?

MINUTES OF EVIDENCE

TAKEN BEFORE THE SCIENCE AND TECHNOLOGY COMMITTEE (SUB-COMMITTEE II)

THURSDAY 23 OCTOBER 1997

Present:

Ackner, L.
Brain, L.
Carmichael of Kelvingrove, L.
Craig of Radley, L.
(Chairman)
Flowers, L.

Hogg, B.
Howie of Troon, L.
Leicester, L Bp.
Nathan, L.
Phillips of Ellesmere, L.
Tombs, L.

Memorandum by Justice

INTRODUCTION

1.1 JUSTICE is an all-party human rights organisation,¹ seeking to reform the law and its administration in order to protect and raise adherence to human rights standards. We have recently commented on several Government proposals involving the use of new technologies such as the licensing of trusted third parties and computer encryption, the provision of electronic services and the proposals for new data protection legislation. We now welcome the opportunity to contribute to the House of Lords Select Committee's present inquiry on digital images as evidence.

1.2 Of the questions raised by the Committee in its letter calling for evidence, we wish to comment on the following:

- What is the state of current technology for collection, storage and transmission of images by digital means, and what are its likely applications?
- What is the state of the art in digital image manipulation, and what safeguards are necessary against misuse of such technologies, especially in relation to digital images being adduced in evidence?
- Does use of CCTV cameras, especially when combined with digital imaging techniques, interfere with human rights, and if so, should there be special safeguards?

COLLECTION, STORAGE AND TRANSMISSION OF IMAGES BY DIGITAL MEANS

2.1 The advent of the digital age has had an immense impact on all areas of life. Film and photography are only a few amongst the many technologies revolutionised. Traditionally, images have been captured and stored on film. Although many copies could be made of photographs, or movies, there was always one "master copy", one original negative.

With the mass computerisation of society witnessed over the last few decades, this is no longer necessarily so. The advent of digital cameras means that images may now be directly captured in digitised form, and stored on digital media such as computer disks. Unlimited numbers of copies may be made without loss of quality; and it is not necessary to keep one "master copy".

2.2 Technology for digitally capturing and storing images, even state of the art, comes cheaply; digital photo cameras are offered at manufacturer's prices starting at £180 for a complete package,² while digital video cameras start at £1,400.³ "Scanners" that read and digitise photographs stored on traditional media, such as film, can be bought for prices as low as £69.⁴ High street prices for a modern personal computer which can handle digital images comfortably start at £1,000.

2.3 In order to transmit digital images at high speeds, transmission systems such as fibre-optic cables are necessary. It is understood that the current state of development of such systems already provides adequate capacity to cover most commercial applications. British Telecom, for one, advertises that its "ISDN" digital lines can be set up at short notice. Although BT are the leading providers, cable networks are also laid by (and can be leased from) organisations such as Railtrack and British Gas.

¹ In preparing this Report, JUSTICE has been greatly assisted by Caspar Bowden, Principal Consultant, Qualia Internet Consultants, and Dr Clive Norris, Centre for Criminology and Criminal Justice, University of Hull.

² The Kodak DC20; price quoted is US recommended retail price. The similar Casio QC10A1 sells at a UK high street price of £299.

³ The JVC GR DVJ70.

⁴ The PRIMAX hand-held scanner.

23 October 1997]

[Continued]

2.4 The likely applications of digital imaging and digital transmission technology are manifold. One of the most important and interesting applications for law-enforcement purposes is the capacity for digital street surveillance cameras (CCTV cameras) to be linked with central data bases containing personal information. For instance, a digital CCTV system connected to a data base containing individuals' passport photographs would enable instant automated facial recognition and identification of individuals captured on CCTV. This is discussed in detail below.

IMAGE MANIPULATION

3.1 Traditional image manipulation techniques involve retouching the original negatives of photographs or film. Examples can be found in the official history-books of the former Soviet Union: famous is an early picture of Lenin speaking on the Red Square in Moscow, with Leon Trotsky, then one of his main aids, clearly visible in the foreground. However, after the Russian revolution, Trotsky fell from grace, and was eventually exiled. Because Lenin no longer wanted to be associated with him, he had him airbrushed out of this and many other pictures in an attempt to re-write history.

Over the years a high level of sophistication has been attained in the "art" of retouching film-based photographs. However, it has never been brought to perfection: to the eyes of an expert, the tell-tale flaws are always there.

3.2 Digital imaging, and digital image manipulation, has brought with it a whole new range of possibilities. Aspiring "forgers" are no longer restricted to crudely tampering with negatives; instead, they now have the possibility to "play" with the very building blocks of computer images, the so-called "pixels". These are the little "dots" that together make up every computerised, or digitised, image. Tampering with these leaves no physical trace and, if done with expertise, a "fake" image is indistinguishable from a real image. The computer packages available mean that even a lay person can readily attain a relatively high level of sophistication in such techniques.

GUARANTEEING AUTHENTICITY

3.3 As digital manipulation of photographs is undetectable the possibility for misuse is great, especially where the original image is taken on a digital camera and no negative exists. This need not necessarily be deliberate misuse; enhancing techniques such as those currently in use for the identification of car number plates can be surprisingly accident-prone. Car number plate enhancement could work through using a programme which vertically connects all black dots within a certain area. Thus, sharpening a blurred P that has lost part of its curve may turn it into an I, while a horizontally sharpened F could turn into a B.⁵

3.4 We consider that there are two ground rules that need to be considered in preventing misuse of digitally enhanced or manipulated images:

- First, as a general rule, the enhancement of a digital image should not add anything to the image: it should merely expose that which is already latent in the image. This is particularly important in relation to enhancing processes as used for car number plate recognition (see above).
- Second, in those exceptional circumstances, where enhancement is necessary in order to sharpen an image, for example, every step taken in the process must be recorded. It should be made clear that in these circumstances the enhancement is effectively an "interpretation" of the image. To implement this rule it would be necessary to require that all enhancement software make provision for such a record; the Home Office's enhancement software, "Home Office Improve", is an example of how it works in practice.

In addition, it has been suggested that the same technology which provides for digital capture, storage, manipulation and transmission of images should also provide a solution to the problem of proving authenticity. Broadly, as an alternative to handing over an unretouched original negative, two suggestions are being made: digital watermarking and the encryption of images.

WATERMARKING

3.5 A digital watermarking system would embed an imperceptible, digital watermark in any image.⁶ While not apparent to the human eye, this watermark is still readable even after an image has been edited, or printed and re-scanned. The watermark consists of an algorithm altering the spatial frequency characteristics of the image, which persist even after re-processing procedures such as scanning and manipulating.

⁵ For a detailed account see P Plowden, M Stockdale, D Elliot, "New techniques and new devices", *New Law Journal*, 4 April 1997, pp 502-504.

⁶ In-camera verification systems can be seen as another form of watermarking. Such systems would super-impose a time/date/serial-number stamp on an image.

23 October 1997]

[Continued

On a commercial basis, digital watermarking schemes are already being marketed for copyright protection purposes. One of the industry-leaders in digital image manipulation, Adobe, offers watermarking software to protect the copyright of images manipulated with its Photoshop software.

The disadvantage of such a scheme is its attractiveness to computer “hackers”: individuals who make it their hobby to break into (high security) computers. As, up to now it has proved impossible to design “hack-proof” computer systems, expectations for a tamper proof watermarking scheme cannot be great. At the same time, the (inadvertent) leaking of the watermarking algorithm to a third party may pose an even greater risk. Once this algorithm is known to outsiders, in principle any watermark can be removed and re-applied.

ENCRYPTION

3.6 Another method suggested to establish the authenticity of digital images is through an encryption procedure. If, upon capture, the digital code for an image is encrypted, the image cannot be tampered with without access to the encryption key which is kept in a safe place. To an extent Kodak is already marketing such a scheme through the use of a file-code for its digital cameras: only the original Kodak camera can produce the code. Although the code can be read by manipulation software, such as the Adobe Photoshop package mentioned above, its software cannot save a file in the Kodak patented format. Certainly for the time being, therefore, an image presented in the Kodak format has probably not been tampered with.

However, as with watermarking, encryption is unlikely to provide a fully tamper resistant safeguard. For example, the code format used in the Kodak digital cameras is not in fact regarded as a particularly strong form of encryption. Although only a few software programs are currently capable of reading the format, the possibility of designing software which can read and write the format is said to be relatively straightforward.

Even if it is possible to develop strong, tamper-proof encryption methods there remains the problem of ensuring that the image is not tampered with prior to encryption. To overcome this, it would be necessary to require that approved encryption software is incorporated within the camera. This raises the practical problem of agreeing global standards for approved encryption software in relation to digital photography.

As with the possible leaking of the watermarking algorithm, the weakest link in an encryption scheme is key-security. Adequate security systems would need to be devised including tamper-proof protocols for the electronic exchange of keys. We understand that these are proving difficult if not impossible to design.

3.7 JUSTICE concludes that, at the present time, technology alone is unlikely to provide the necessary protection against misuse of digitally manipulated images. Although there is a strong case for continuing research into uniform, robust watermarking and encryption schemes, building confidence in the fool-proof nature of such procedures is a longer-term objective.

ADMISSIBILITY IN EVIDENCE

3.8 The lack of tamper-proof technology does not mean that digital images should be automatically excluded as evidence in legal proceedings. It would be both unrealistic and impractical for courts to disregard the increasing use of digital cameras and digital storage of images. Not to admit such material in evidence would be to ignore large amounts of photographic material with potential relevance to the proceedings. As the Court of Appeal said in a 1966 criminal case, it would be “wrong to deny the law of evidence advantages to be gained by new techniques and new devices”.⁷ The question is therefore what evidential procedural requirements, including the use of technology, are necessary in order to ensure that digital-image evidence is sufficiently reliable, particularly in terms of identification evidence.

The courts have already developed a set of strict procedural requirements to establish the authenticity of traditional film-based images. JUSTICE believes that digital image evidence should be subjected to a similarly strict level of scrutiny but one which reflects the additional risk of undetectable manipulation. This means requiring the use of approved security measures in the gathering and storage of digital images as an additional way of proving authenticity of the image, particularly in relation to criminal proceedings.

We therefore propose that those wishing to adduce digital image evidence in legal proceedings should be required to show:

- *a chain of custody*. This means identifying the origin and history of the image up to the moment of its production in court.⁸ Where enhancement software is used, every step of the enhancement process must be recorded and documented. As mentioned above at para. 3.4, enhancement should only expose what is already latent in the image and not add to it.
- In order to establish this chain, there will need to be a statement by the original photographer testifying as to its authenticity and describing the time, place and circumstances under which it was

⁷ *R v Ali (Maqsood)* [1966] 1 QB 688.

⁸ *Cf R v Robson and Harris* [1972] 1 WLR 651.

23 October 1997]

[Continued]

taken; and a statement relating to subsequent storage.⁹ These should include a declaration regarding the proper use of any computer equipment analogous to Section 69 of the *Police and Criminal Evidence Act 1984 (PACE)*.

- *the security measures used.* This means identifying the security system or systems used to ensure the authenticity of the image, including watermarking and encryption. It will be necessary to have an up-to-date list of approved systems available to the court. In the absence of an approved or any security scheme being used, the court should have the usual discretion of excluding the evidence on grounds of unreliability.

4. CCTV AND HUMAN RIGHTS

4.1 The use of CCTV systems has become widespread over the past decade. They are used in places like town centres, shopping malls and parking lots. In the main, public perception is that they increase security. Although the value of CCTV in preventing crime is by no means a proven fact, their popularity continues. The Home Office CCTV Challenge Competition for 1997–98 attracted a total of 188 bids, involving the installation of 2298 new cameras. Trade magazines estimate the total UK market to be worth £300m.

4.2 CCTV systems, used in conjunction with digital imaging and data retrieval techniques, offer unique surveillance opportunities. It facilitates, with the use of computer based storage and analysis software, the identification of people and vehicles en masse, as they move through public space. Three related technological developments promote this possibility:

- the introduction of high speed/high volume digital transmission systems such as fibre optic cables;
- the development of a new generation of sophisticated database products which can link existing databases; and
- the rapid development of image manipulation and pattern recognition software.

Automatic licence plate identification and matching are now routinely achieved through the use of digitised images and advance pattern recognition software. Automatic facial recognition software is also beginning to enter the commercial market with software which automatically compares ‘captured’ faces with those held on a computer database.

CURRENT APPLICATIONS

4.3 A full description of existing CCTV and facial recognition systems are attached in an appendix. The following are particularly important examples:

4.4 The “*Ring of Steel*” system maintained by the City of London Police Force consists of ninety CCTV cameras recording the movement of all traffic in and out of the square mile of the city. Twenty eight of these security cameras are installed at eight official entry points. The camera lenses are capable of preventing wide screen glare and reflection, and clearly identify the occupants of the car and the vehicle registration plate.¹⁰ In May 1996, the capacity of the system was significantly enhanced with the addition of automated licence plate recognition. This creates a database of the licence plates of all cars entering and exiting the area. Any vehicle which does not exit the system after a specified time automatically triggers an alarm which alerts the operators to the presence of a suspect vehicle. Additionally, all the licence plates are held on a computerised database which can be automatically run against any number of other databases; for example, an index of stolen cars or the vehicles associated with known suspects. The system currently checks over 100,000 vehicles each day.

It was announced in July this year that the Metropolitan Police are planning to introduce Automatic Licence Plate recognition throughout the capital¹¹ and that Customs & Excise are installing similar technology to log the licence plates of every vehicle entering the UK. Meanwhile the DVLA is planning to invest in a nationwide system of cameras to identify untaxed cars being driven on the roads; data from these cameras will be shared with the police.¹²

4.5 Software & Systems International, are carrying out trials of their Mandrake system in the *Watford City football stadium*. This is a fully automated facial recognition system, which scans the faces of the crowd in “real” time and compares the faces with images of known “troublemakers” held on a digital database. The initial trials have been successful and the system is expected to become fully operational later this year.¹³

⁹ For instance *R v Dodson, R v Williams* (1984) Times, 14 April.

¹⁰ *The Guardian*, 24 November 1993.

¹¹ *The Independent*, 22 July 1997.

¹² *Sunday Telegraph*, 15 September 1996, p 9.

¹³ *Computer Weekly*, 24 July 1997.

23 October 1997]

[Continued

FUTURE APPLICATION

4.6 Within the limits of current technical development, automatic facial detection has been shown to work best with "restricted types of data and data that has been carefully structured".¹⁴ For example, rather than producing a definitive single match, the four most likely faces will be identified, with the human operative making the final judgment. However, predictions suggest that reliable automatic recognition systems will increasingly be developed.

4.7 The actual usefulness of facial recognition systems depends on the existence of other databases which identify individuals. While the DVLA holds all vehicle registrations linked to named individuals, there is as yet no national archive of named faces. This means that systems such as Mandrake can only be used to locate already known offenders within a crowd. However, this is likely to change in two respects. First, the new Drivers Licence with an attached photograph is almost certainly going to be held in digital form;¹⁵ and second, the Passport Agency has announced a move towards a similar digital system for applicants' photographs.¹⁶

4.8 All the signs are that the prospect of being able to match a face from a city centre surveillance scene with one held on a computerised data base is rapidly advancing. Although it is difficult to predict when this is likely to be achieved, there are two factors which make it a highly attractive option. First, the cost of human monitoring of CCTV is huge. For example, monitoring a medium-sized town centre with twenty to thirty cameras for a 24-hour period requires at least ten staff at a cost of around £100,000 per annum. Digitised systems which utilise automatic event recognition can be monitored from remote centralised control rooms by only one staff operator. Second, the speed at which Automatic Licence Plate recognition has moved from the drawing board to implementation has been rapid: following the promise of such applications in 1989, they were commercially available by 1993. Four years later there are at least 24 companies selling "off the shelf" automated systems.¹⁷ The majority of the systems have been for road tolling systems but, as we have noted above, the law enforcement and security applications are rapidly emerging. In the case of CCTV, one of the leading industry commentators recently stressed that "the future is in digital CCTV working on a digital super-highway."¹⁸

HUMAN RIGHTS IMPLICATIONS

4.9 The combination of digital photography, image recognition and matching software brings with it the prospect of a mass surveillance society—a society in which movements and interactions in public spaces are regularly monitored, recorded and logged. There is a real prospect that public and civic life can no longer be viewed as carrying with it an expectation of anonymity. Every journey, meeting and encounter will be potentially capable of being officially recorded, stored and matched to other centrally held records: social security, health, tax and criminal records, to name but a few.

4.10 The human rights implications are therefore potentially serious. Most obviously, there is the interference with privacy rights protected through such instruments as the European Convention on Human Rights and the International Covenant on Civil and Political Rights,

Article 8 of the European Convention provides:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

4.11 In its case law, the European Commission of Human Rights has affirmed that privacy rights may, in certain circumstances, be asserted in public places.¹⁹ This is especially so in relation to the exercise of other rights, such as the right to freedom of expression and assembly, when the use of CCTV cameras may have a "chilling" effect. People may be unwilling, for example, to participate in lawful demonstrations if this is to be recorded on CCTV.²⁰

Interference with privacy rights may also arise from the use and retention of CCTV footage. The information recorded may touch closely on the private life of individuals. An extreme example of this was provided in 1995, with the publication of a video containing extracts of CCTV footage obtained from private

¹⁴ G Robertson, I Crow, "Testing facial recognition systems", *Image and vision computing*, Vol 12 No 9, pp 609-614.

¹⁵ Davies 1996, 196.

¹⁶ *Computer Weekly*, 3 July 1997.

¹⁷ *Traffic Technology International*, June/July 1997, pp 105-110.

¹⁸ John Comfort, *CCTV Today*, May 1996.

¹⁹ *Friedl v Austria*, European Court of Human Rights (1995), EHRR Series A No 305 (friendly settlement). For more on this, see D Feldman, *Privacy-related rights and their social value*, in Birks (ed), *Privacy and loyalty*, Oxford University Press, Oxford 1997.

²⁰ This was the case in *Friedl v Austria*, above.

23 October 1997]

[Continued]

security firms which included shots of people participating in sexual activities in elevators and undressing in changing rooms. More recently has been the case of an attempted suicide being recorded on CCTV and subsequently published.

The future development of combining digital CCTV systems, with facial recognition techniques and other digital data bases at the touch of a button, adds a major new dimension to the need for safeguards.

SAFEGUARDS

4.12 The second paragraph of Article 8 ECHR sets out the circumstances under which the right to respect for privacy may be limited. Interferences must be in accordance with the law, in pursuit of a legitimate aim and “necessary in a democratic society”. In its case law,²¹ the European Court has crystallised these abstract principles into the following safeguarding requirements:

- legislation (or express common law powers) are a necessary prerequisite for any interference;
- this legislation must be sufficiently precise to enable individuals to foresee in what circumstances their rights may be interfered with;
- it must provide safeguards against abuse of powers;
- the interference must be proportionate to the aim pursued; and
- if the interference is in pursuit of law enforcement purposes, then other means must have been tried and failed, or are unlikely to succeed.

4.13 Until the ECHR is incorporated into domestic law, the main legislation safeguarding privacy rights is the 1984 Data Protection Act (the DPA). Although its provisions can apply to CCTV footage when the data is processed automatically by reference to an identified individual, the Act was not drafted with the complexities of CCTV in mind. For example, it is of limited use in providing safeguards against full-scale data sharing between different agencies as envisaged by the development of facial recognition systems.

For the purpose of this report, we have divided the question of safeguards into two main areas. First, there are the wider issues concerning the licensing of CCTV systems, their overall management and accountability. These are clearly identified in the voluntary code of practice published by the Local Government Information Unit (LGIU).²² Although we have not considered these matters in detail, we believe that increasing use of CCTV and its potential development as a form of widespread surveillance indicates the need for a regulatory framework.

Second, there are the individual privacy issues, including disclosure and data sharing, access and retention of CCTV footage which specifically raise data protection safeguards. These are areas which JUSTICE has considered in some detail.

EC DATA PROTECTION DIRECTIVE

4.14 The question of providing adequate data protection controls over sound and image data is referred to in Recitals 14 to 17 of the preamble to the EC Data Protection Directive (95/46/EC). They make it clear that such data must be covered under certain conditions, with specific mention of video surveillance (CCTV). Despite this, the Government’s recent proposals for implementing the Directive into UK law make no mention of the scope of the Directive regarding sound and image data.²³

Although, Recital 16 and Article 3 exclude from the scope of the Directive activities such as “public security, defence, State security... and the activities of the State in areas of criminal law”, we do not believe that this excludes all forms of CCTV in public places. In any event, since the proposed Data Protection Bill is designed (like the 1984 Act) to cover law enforcement activities which are outside the scope of Community law, there is no valid reason for following the exclusions contained in the Directive.

In our view, the forthcoming Bill provides the best opportunity for ensuring that privacy rights of individuals in relation to CCTV data are fully protected under data protection laws. We believe that this is particularly important in light of the imminent incorporation of the ECHR into UK law.

We now consider two areas where the lack of adequate safeguards gives rise to particular concern.

²¹ See for instance *Malone v UK* (1984), European Court of Human Rights, Series A No 82; *Sunday Times v UK* (1979), European Court of Human Rights, Series A No 30.

²² *A Watching Brief—A Code of Practice for CCTV*, LGIU (March 1996).

²³ *Data Protection: The Government’s Proposals*, Home Office (Cm 3725), July 1997; *Response by JUSTICE to the Home Office paper*, 21.8.97.

23 October 1997]

[Continued]

DATA SHARING AND DATA MATCHING

4.15 Data matching is essentially the sharing and comparing of data collected by different agencies for different purposes. Such exercises are now widely in operation in both the public and private sectors, particularly in relation to detecting fraud. Although the Data Protection Act places restrictions on the disclosure and use of personal data for a purpose different to that for which it was collected, data matching can come within its provisions when:

- the exercise takes place on a statutory footing and is therefore “required by law”. The recent 1997 Social Security Administration (Fraud) Act which provides for the sharing of information between a number of government departments is an example of this; and
- the exercise is for the prevention or detection of crime, the apprehension or prosecution of offenders or the assessment or collection of any tax or duty. As the Data Protection Registrar has pointed out, this is exercisable only on a case by case basis and does not cover the wholesale disclosure and matching of personal data which is often a feature of data matching initiatives.²⁴

While we accept that there is a legitimate interest in law enforcement agencies having access to CCTV data for the purposes of a criminal investigation in certain situations, it is clear that the present Data Protection Act is not designed to cover wide, data matching exercises as envisaged by the development of facial recognition systems.

4.16 The issues raised by large data matching activities, particularly in the public sector, have been the subject of specific legislation in a number of countries. Canada, the USA, Australia and New Zealand have all introduced data matching laws to regulate the balance between what is required in the public interest to detect fraud, for example, and the rights of individual citizens. In general terms, this is achieved by placing limitations through a Code of Practice on those conducting data matching exercises.

The Data Protection Registrar has emphasised the need for similar regulation in this country. For example, she called for a statutory Code to be established for central government data matching activities arising from the Social Security (Fraud) Act mentioned above. We believe that an even stronger case can be made out for controlling data matching of CCTV footage.

INDEPENDENT SCRUTINY

4.17 Independent scrutiny is necessary in order to ensure compliance with the Data Protection Act. At present, the Data Protection Registrar may only investigate after a complaint has been lodged or an offence is suspected. She does not have independent powers of audit to spot-check compliance with the law. Our limited enquiries concerning other member states reveal that the UK is exceptional in its omission to have auditing powers. In Germany, the Netherlands, Spain and Sweden the data protection authorities have full powers to audit data processing in both private and public sectors (including the police). Authorities in most other member states have at least a general power to conduct investigations on their own initiative.

Again, the Government's proposals for implementing the EC Directive fail to give effective powers of data protection audit to the Registrar. We believe this to be contrary to the intentions of the Directive and leaves in doubt the Registrar's powers to carry out her supervisory duties under such intergovernmental conventions as that governing Europol. It is an omission which is especially relevant in view of the rapidly growing capacity of public agencies to amass and exchange personal data. The kinds of technology development discussed in this report place even greater emphasis on the need to increase such powers.

CONCLUSIONS AND RECOMMENDATIONS

The likely applications of digital imaging and digital transmission technology are manifold. In terms of law enforcement, the development of CCTV digital cameras linked to central databases containing personal information would enable instant automated facial recognition and identification of individuals. However, digital imaging brings with it particular dangers; first, the ease of processing undetectable digital manipulation of images creates the possibility of serious misuse; second, the prospect of widespread surveillance through CCTV systems endangers the privacy rights of individuals.

GUARANTEEING AUTHENTICITY OF DIGITAL IMAGES

Tampering with digital images leaves no physical trace and, if done with expertise, a “fake” image is indistinguishable from a real image. Misuse of an image need not necessarily be deliberate: enhancing techniques such as those currently in use for the identification of car number plates can be accident-prone. The use of approved security measures in the gathering and storage of digital images, together with ground

²⁴ See *A Guide to developing Data Protection Codes of Practice on data matching*, Data Protection Registrar's Office, August 1997; *Private Lives, and Public Powers*, DPR July 1997.

23 October 1997]

[Continued]

rules on enhancement procedures, are necessary requisites for guaranteeing the authenticity of a digital image.

JUSTICE recommends that digital image evidence in legal proceedings should be subjected to a strict level of scrutiny. Those wishing to adduce such evidence should be required to show:

- a chain of custody to identify the origin and history of the image up to the moment of its production in court. Any enhancement procedure should only expose what is already latent in the image and not add to it. Every step of the enhancement process must be recorded and documented; and
- the security measures that have been used to ensure the authenticity of the image, including such processes as watermarking and encryption. An up-to-date list of approved systems needs to be available to the court.

SAFEGUARDING HUMAN RIGHTS

The prospect of being able to match a face from a city centre surveillance scene with one held on a computerised data base (such as those proposed under the DVLC and the Passport Agency) is rapidly advancing. The human rights implications, particularly in terms of infringing privacy rights as guaranteed by Article 8 of the European Convention on Human Rights, are potentially serious. The forthcoming Bill to implement the EC Data Protection Directive provides the best opportunity for ensuring that there are satisfactory safeguards to protect individual privacy. JUSTICE recommends that:

- data protection legislation as amended by the proposed Data Protection Bill should unambiguously cover CCTV data including individuals' rights over use of the data;
- wholesale data matching activities in relation to CCTV data should be the subject of statutory control through a Code of Practice;
- the Data Protection Registrar should be given independent audit powers of inspection. This is especially relevant in view of the rapidly growing capacity of public agencies to amass and exchange personal data; and
- the potential development of CCTV as a form of widespread surveillance also indicates the need for a regulatory framework to cover such issues as the licensing of CCTV systems, their overall management and accountability.

APPENDIX 1

CURRENT APPLICATIONS OF DIGITAL CCTV TECHNOLOGY²⁵

DOLLAND'S MOOR

The EDS system installed at Dolland's Moor, the Channel Tunnel rail freight marshalling yard, currently monitors input from 48 cameras. Through the use of digitised cameras, microcomputers and neural network technology the computer system learns the features of a scene and to detect changes to it. Rather than relying on remote sensors, this intelligent image processing system can detect up to six events in any one scene, merely by analysing the information provided by the incoming pictures. Through the use of algorithms to interpret the images, a system can react to motion or non motion; to object size, speed and direction; to duration in an area; and direction of exit and entry. What this means in practice is that such systems can automatically monitor complex scenes and trigger alarms and other security mechanisms when unsanctioned events occur. For instance, a stationary vehicle can trigger an alarm, as can a person heading in the "wrong" direction. (EDS 1995)

The intelligent image recognition ability of these systems enables them to be, "highly discriminatory and to raise alarms only when objects that satisfy all of the rules are detected on the scene." Whereas light or pressure sensors are triggered when anything breaks the circuit, such as a rabbit or bird, intelligent systems will ignore these on the basis of a size discriminator algorithm. Similarly, the presence of a person loitering in a specific location, even in a busy street, can be identified through tracking and dwell time algorithms which will successfully discriminate between loiterers and passers-by (Signal; July 1995).

At Dolland's Moor, without a physical responsibility for monitoring the screens there is only a need for one operative to be on duty at any one time to respond to system triggered alarms.

THE "RING OF STEEL", CITY OF LONDON POLICE

The system consists of 90 CCTV cameras recording the movement of all traffic in and out of the square mile of the city. 28 of these security cameras have been installed at the eight official entry points to the Square Mile. The camera lenses are capable of preventing wide screen glare and reflection, and clearly identify the

²⁵ Kindly provided by Dr Clive Norris, Centre for Criminology and Criminal Justice, University of Hull.

23 October 1997]

[Continued

occupants of the car and the vehicle registration plate (*The Guardian* 24 November 1993). In May 1996, the capacity of the system was significantly enhanced with the addition of automated licence plate recognition. The system creates a database of the licence plates of all cars entering and exiting the area. Any vehicle which does not exit the system after a specified time automatically triggers an alarm and alerts the operators to the presence of a suspect vehicle. Additionally once all the licence plates are held on a computerised database they can be automatically run against any number of other databases; for instance, an index of stolen cars or the vehicles associated with known suspects. At present the system checks over 100,000 vehicles each day.

It was announced in July this year that the Metropolitan Police are also planning to introduce Automatic Licence Plate recognition throughout the capital (*Independent* 22 July 1997) and that Customs are installing the technology to log the licence plates of every vehicle entering the UK and the DVLA is planning to invest in a nation wide system of cameras to identify untaxed cars being driven on the roads and that data from the camera will also be shared with the police (*Sunday Telegraph* 15 September 1996, p9).

CENTRAL SCOTLAND POLICE

Central Scotland Police for example are currently installing a new force intelligence system based on Memex's computerised database handling software. This software not only enables the integration of all existing force and even external databases, but can hold visual and audio data too. As was made clear by the Chief Constable, the purpose of this new system is to facilitate a massive expansion of the intelligence capacity of the force: "What do we class as intelligence in my new system in the force? Everything: the whole vast range of information that comes into the possession of a police force during a 24 hour period will go on to my corporate database. Everything that every person, vehicle is associated with..." (SciFiles BBC2 March 1996).

THE FOOTBALL INTELLIGENCE SYSTEM

This has been developed by the Greater Manchester Police Football Intelligence Unit and consists of a lap top computer running a "windows database". The system collates information and photographic records of suspects and offenders associated with football violence and is used at Manchester City's Maine Road ground. From a set of personal descriptors entered by the operator the system will display the pictures of the 12 most likely suspects from a database of 150 "known" offenders. Details can be cross referenced with details relating to previous convictions, intelligence information, "hooligan" associates, and gang membership.

NATIONAL CRIMINAL INTELLIGENCE SERVICE'S DATABASE

This holds details and pictures of 6,000 suspected football hooligans which in the run up to the 1996 European football championship, which was made available to all the participating football grounds through the use of "photo-phones" enabling digitised photographs to be transmitted from one central location to a remote terminal in each stadium (*The Guardian*, 10 February 1996).

PUBLIC ORDER UNIT OF THE METROPOLITAN POLICE

The Unit is now deploying Kodak Digital cameras at demonstrations. The system is being used to digitally photograph demonstrators, and immediately relay the image to operational units so as to identify and detain troublemakers as they leave the area. (Hook; 1994 11).

DECTEL'S CRIME NET

At present the system is being used to compare digitised photographs of unidentified Building Society robbers against a database of known offenders. The system is as yet only semi automatic. Each face is coded manually according to the distinctive spatial relationships between key points (such as the corner of the mouth and the bridge of the nose). This is said to give each face a unique identifying code. As new faces are added to the database for identification, they are measured, and then automatically compared with the other images. The system has been piloted by the Metropolitan Police's Flying Squad, and Dectel aims to market the system for use by retailers to identify shoplifters and in town centre surveillance systems.

WATFORD CITY FOOTBALL STADIUM

Software & Systems International, are carrying out trials of their Mandrake system, which is a fully automated facial recognition system based on neural network software. The system scans the faces of the crowd in "real" time and compares the faces with images of known "troublemakers" which is held on a digital database. The initial trials have been successful and the system is expected to become fully operational later this year. (*Computer Weekly*, 24 July 1997)

23 October 1997]

[Continued]

Evidence of Liberty and the University of Northumbria at Newcastle²⁶

Q1. What is the current and forecast future use of digital technology for image collection, storage and transmission? What is its use by the courts and the legal profession? What is the state of the art of image manipulation?

1. In the context of criminal proceedings, the main types of video recorded evidence will be:
 - (i) recordings made by surveillance or security cameras; and
 - (ii) the video recorded testimony of witnesses (as permitted by statute).

In the future, video recordings of police interviews are likely to become increasingly common. Video evidence has also been ruled admissible where it has contained recordings of the re-enactments of crimes.

2. Video recordings may also be of relevance in civil proceedings. An example of this would be where a defendant to personal injury proceedings wishes to use covert video footage to prove that the consequences of the plaintiff's injuries are not so serious as the plaintiff alleges.

3. At present the majority of recordings will still be analogue, although digital enhancement may have taken place by the time a recording is viewed by a court. Enhancement is most likely to have taken place in the context of recordings by surveillance or security cameras. In the future, as the ease of storing digital images increases and digital technology becomes more widely used for surveillance or security purposes, the proportion of digital as opposed to analogue recordings will presumably increase.

Q2. Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean that they should be treated differently when used as evidence?

4. The question concerns the "different" treatment of video evidence, the "difference" presumably being from the treatment of other forms of evidence. Although the question focuses on the ease of tampering, presumably what is of equal concern is the difficulty of detecting any such manipulation in digital images. The question also refers to the ease of copying such images. Here the concern will be that while tampering with an image will often be detectable at bit level in that image, when the tampered image is copied there will be no evidence on the copy of any break in the underlying continuity. While with analogue images, the loss of quality in any copy will often indicate that an image is not the original, this is of course not the case with digital images, so that it may prove impossible to determine whether an image is original or not.

5. While the courts have been eager to use video-recorded images as evidence because of their high probative value, they have not conclusively determined the status of video images as evidence. While the courts have indicated that video footage (whether analogue or digital) is akin to tape-recordings²⁷ and is to be treated no differently from still photographic images, it has been said both that a video recording is a form of real evidence²⁸ and that it is a form of evidence in a class of its own.²⁹ In either event, the courts have made clear that the best evidence rule (which historically required originals of documentary evidence to be put before the court) does not apply to video-evidence.³⁰ There is therefore no requirement to certify to the court that the images put before it have not at some stage—or indeed, a number of stages—been copied.

6. The question refers to the difficulty of maintaining an audit trail. Two points can be made. First, an approved software package such as Home Office Improve (or Improve 2) will provide such a trail, but it will of course only record the manipulation of the image while subject to that software; it cannot confirm that it is working with an original and previously unmanipulated image. Secondly, even where a clear audit trail exists, this will only provide a route for a second technician to follow in order to determine what modifications have taken place to the image. Of itself, the audit trail will mean nothing to non-experts, such as defence lawyers or the courts. An audit trail will therefore only assist if the other party or the court has the facilities to assess the manipulation process itself.

7. Should digital video evidence therefore be treated differently because of this difficulty in assessing whether manipulation has taken place and what form that manipulation has taken?

8. At common law, video recorded evidence does not fall within any general rule of exclusion (such as the rule excluding hearsay evidence). It may be proved by a copy, regardless of the number of removes between the original and the copy, or by the oral testimony of a witness who viewed the video recording. Expert witnesses may be called where they can provide relevant expertise which the court lacks (for example in relation to matters such as facial mapping). More controversially, non-expert witnesses may be permitted to assist the court to interpret video recordings where they possess a familiarity with the material which the

²⁶ Compiled by Philip Plowden, solicitor and principal lecturer, Dr Michael Stockdale, senior lecturer, both of the University of Northumbria at Newcastle, and Philip Leach, solicitor and legal officer at Liberty.

²⁷ *Fowden v White* [1982] Crim LR 588.

²⁸ *Clarke* [1995] Cr App R 425.

²⁹ *Cook* [1987] 1 QB 417.

³⁰ *Kajala v Noble* (1982) 75 Cr App R 149.

23 October 1997]

[Continued]

recording contains which it would take the jury an unreasonably long time to develop (for example, in cases where police officers have viewed poor quality or confused video images a large number of times).³¹

9. However, video recorded evidence will not automatically be admissible. First, in order to be admissible, evidence must be relevant. Thus, where the quality of a video recording is so poor that the recording is of no value to the court, the evidence may be inadmissible on the basis that it is of no relevance. Secondly, even where video recorded evidence is relevant, a criminal court possesses a general discretion to exclude prosecution evidence the admission of which would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it or the probative value of which is exceeded by its prejudicial effect. Such exclusion might, for example, be justified where the quality of a video recording is poor and the jury might attach a greater weight to it than is properly justified. (It appears, however, that a civil court does not possess any such exclusionary discretion, though the existence or non-existence of exclusionary discretion in civil proceedings has never been conclusively determined.)

10. The most fundamental modification therefore would be to render video evidence, or merely digital video evidence, inadmissible in legal proceedings. It is submitted, however, that since such evidence may frequently be both reliable and highly probative, this would be an undesirable development.

11. A second possibility would be to render such evidence inadmissible subject to exceptions. Such exceptions might relate, for example, to the source of the relevant evidence, to watermarking or to the probity of its audit trail. Again, however, such restrictions might result in the exclusion of reliable and highly probative evidence and, moreover, in the latter two cases, their value is dependent upon the possibility of producing tamper-proof watermarking or a tamper-proof audit trail.

12. A third possibility would be to impose specific requirements of proof in relation to such evidence, for example, to require production of the original and every level of copy/enhanced version as a condition of admissibility. Again, however, the value of such requirements is dependent upon the possibility of conclusively determining whether that which is produced as an original is in fact the original.

13. A fourth possibility is to require some form of direction to the tribunal of fact as to the uncertain reliability of the image. At present, where a witness testifies in relation to the content of a video recording which he has viewed, the jury should be directed in relation to his evidence as they would be in relation to the evidence of a normal identification witness (with the giving of a *Turnbull*³² warning to the jury concerning the dangers of a positive but mistaken identification). In a video case that direction should be modified to take into account both problems relating to the positioning of the camera and problems relating to the recording or copying of the image³³. Where the jury themselves are asked to make an identification from a video recording in the absence of identification witnesses, the courts have stated that a more limited form of direction is required³⁴.

14. Alternatively, rather than simply warning the jury, the judge could be required to direct the jury that supporting or corroborating evidence was required prior to conviction upon the basis of evidence in the form of a digital image. The existence of such a rule might, however, prevent conviction in the context of reliable and highly probative video evidence and, moreover, the imposition of corroboration requirements is now regarded both by the judiciary and by the legislature as imposing undesirable complexities in the context of jury trial. It might, however, go some way to offset the problem that giving the jury a warning or modified *Turnbull* direction in practice does little to offset the disproportionately persuasive power of video evidence which arises from the sense of having witnessed a matter for oneself.

15. Finally, it should be noted that, in criminal proceedings, the admissibility of statements contained in computer produced documents is already subject to statutory restrictions concerning both the proper use of the computer and its proper operation (section 69 of Police and Criminal Evidence Act 1984). The relevant statutory provision might arguably be treated as applicable to digital images but recent case law has rendered both its ambit and the consequences of its application of limited significance by confining the provision to certification as to whether the computer operated properly and not the reliability or otherwise of information generated by the computer.

16. In practice, the ideal position is clearly one in which the probity of evidence in the form of digital images can be determined for the purposes of the court. To some extent this position might be attained in the context of criminal proceedings by ensuring that, where the authenticity of a digital image is challenged, the defence have available to them experts of equal standing to those available to the prosecution. Even this position would be unsatisfactory, however, in that it might not be possible to ascertain whether either or both experts had in fact had access to the original material. Further, it would still be for the jury to determine which expert's evidence to accept, a decision which might at times have little to do with the relative reliability of the

³¹ *R v Clare and Peach* [1995] 2 Cr App R 333.

³² *Turnbull* [1977] QB 224.

³³ *Taylor v Chief Constable of Cheshire* [1987] 1 All ER 225.

³⁴ *R v Blenkinsop* [1995] Cr App R 7.

23 October 1997]

[Continued]

relevant expert evidence. Alternatively, were the role of the expert to be handed to a body independent both of prosecution and defence, ie to some form of "court expert", this might present the appearance of handing the issue over to an organ of the state and, perhaps, of failing to give the accused a fair trial.

Q3. Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence? What would be the preferred practical measure?

17. Clearly, any steps which make it possible to determine whether a digital image is original and whether it has been tampered with would greatly increase the reliability of such evidence. Whether it is at present possible to achieve this, however, must be open to grave doubt. Perhaps the most valuable practical measure which could be adopted at present would be the provision of appropriate expert assistance to the defence in circumstances in which the authenticity of a digital image is challenged. However, on a practical level, many cases in which digital video imagery is admitted as evidence are relatively minor matters, such as road traffic offences or small scale shop thefts. Such offences will often not give rise to any entitlement to legal aid under the s.22 "interests of justice" criteria, and even in those cases where legal aid is granted, the court is likely to be slow to authorise the extension of legal aid to cover the instructing of an independent expert. This lack of equality of expertise between prosecution and defence undermines the challenges that should properly be mounted to test such evidence within an adversarial system.

Q4. in what circumstances and with what controls should modified or enhanced images be used as evidence:

18. Clearly, enhancement (including the application of techniques such as facial mapping) can increase the weight of evidence, but dangers of distortion or fabrication obviously exist. Simply to exclude all enhanced images could thus result in the exclusion of cogent and reliable evidence. Moreover, it might at times be impossible to determine whether an image presented as an original had in fact been enhanced or modified. A useful example of how images may be properly enhanced so as to produce a number of differing results is the enhancement of images of car number plates, where "sharpening" of the image along the horizontal may produce an F or a T, for example, while sharpening the vertical may equally properly produce a P or an I.³⁵

19. The ideal situation would be one in which enhanced images were presented in the context of a proper audit trail and with appropriate expert witnesses available to the defence. At present, however, it appears to be impossible to place total reliance upon any such audit trail and, moreover, in the majority of criminal cases the defence will not have available to them expert support equivalent to that available to the prosecution. As always, the way in which the trial judge directs the jury in such circumstances may be important.

Q5. Do technologies which compress data or use error correction technology when transmitting it raise special problems?

20. In relation to the former issue, clearly compression will reduce the quality of the image which the court eventually views and thus the weight of the relevant evidence. Consequently, directions to the jury should, where appropriate, draw their attention to the inferior quality of the image. Further, this might ideally be a matter for a defence expert to deal with. Finally, compression removes the possibility of enhancement and from this point of view also may reduce the weight of the image which the court views.

21. In relation to the latter issue, again the use of error correction technology may distort the final image and consequently, again may be an appropriate area for judicial direction and expert evidence. In general, the danger in both of these contexts is, perhaps, less with images which are obviously of poor quality than with images which appear to be of good quality but have in fact been distorted.

22. The question asks whether further advice or training should be provided to law enforcement officers and the courts on the technical limitations of the relevant technology. So far as law enforcement officers are concerned, perhaps the most important matters which should be emphasised are proper treatment of the medium in which the image is stored and upholding the integrity of the audit trail. In relation to the courts, the two most important aspects are the extent to which judges, lawyers, magistrates and juries (as directed by judges) appreciate and understand the limitations and dangers of digital technology and the related issue of ensuring that the facilities available in court for the viewing of digital images are of sufficient quality so as not to detract from the quality of the image viewed.

³⁵ We annex a copy of "New Techniques and New Devices"—video evidence and the criminal courts. (1997) *New Law Journal* Vol 147 502–504 (with Michael Stockdale and David Elliott).

23 October 1997]

[Continued]

Q6. Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?

23. Liberty believes that the use of surveillance cameras, particularly in the absence of statutory or regulatory controls, can threaten civil liberties. It is a fundamental premise when considering the use of CCTV that surveillance does intrude on the privacy of individuals, and that it can contribute towards a perception of pervasive state control over the lives of individuals and contribute to a sense of alienation amongst marginalised individuals and groups.

24. We would acknowledge that CCTV now has a role in the prevention and detection of crime. However, in our view the limited public debate surrounding the use of CCTV has not given sufficient attention to the extent to which surveillance may intrude on people's privacy. There has been a tendency to focus on the public's instinctive fear of crime, and to take for granted the assumption, usually in the absence of reliable evidence, that CCTV reduces crime.

25. Recent research including public opinion surveys has recorded a wide variety of concerns expressed by the general public³⁶ that the wrong conclusions may be drawn from taped evidence; about the impartiality and accountability of the users of CCTV systems; the lack of information about who is watching the public and how video material will be processed and used; the need for restrictions on the use of CCTV to safeguard privacy and protect against discriminatory practices; and the significant increase in surveillance into people's lives and the gradual erosion of civil liberties.

THE PEOPLE AND ACTIVITIES TARGETED BY THOSE OPERATING SURVEILLANCE CAMERAS

26. Liberty is concerned that CCTV may be used to target marginalised individuals and groups, such as travellers, young people, political campaigners, demonstrators, and people from ethnic minorities whose use of public space may conflict with commercial and other conventional views of appropriate and legitimate uses of public space. These groups may be conspicuous and attract the attention of camera operators even though their conduct is not criminal. It is a matter for concern that non-consumers using public spaces may become the target of unwarranted surveillance, reflecting the commercial priorities of major investors in expensive CCTV systems. We would also be concerned that surveillance may be used for purposes which go beyond crime prevention and detection, such as monitoring behaviour perceived to be "anti-social". Moreover, there is evidence that CCTV schemes are being used for purposes quite unrelated to crime prevention, such as to monitor the time of arrival and quality of work of council employees and contractors, and to search out school truants.³⁷

27. The use of image tracking software could have particular adverse effects on civil liberties if such systems were used to detect so-called known offenders, or those who might be known to the police but who had not been convicted of any offence. In our view it cannot be justified to track particular individuals (even those who have had prior convictions) for reasons unrelated to their behaviour at the time of filming.

TRAINING AND SUPERVISION OF CAMERA OPERATORS

28. We would emphasise the need for the training of all camera operators to a sophisticated level, and for their adequate supervision, in order that unwarranted intrusion into people's privacy is prevented. In one recent case, an employee of a private firm contracted to operate the Ogwr Borough Council CCTV system in Maesteg was found to have been zooming in on public telephone kiosks in order to make obscene calls to users.³⁸ In many instances, cameras are being operated by employees of private security firms, which remain unregulated.

HIDDEN CAMERAS

29. Liberty considers that the public should not be covertly filmed. Surveillance systems should be signalled by signs at the perimeter of the area covered by cameras. The signs should indicate in specific language the purpose of the system, the extent of the area covered, the body responsible for overseeing the system and details of who to contact with questions and complaints. Cameras should be large enough to be readily visible.

³⁶ See, for example: *Closed Circuit Television in Public Places*, T Honess/E Chapman, 1992, Police Research Group. Crime Prevention Unit Series Paper 35, Home Office; *CCTV in Town Centres: Three Case Studies*, B Brown, 1995, Police Research Group. Crime Prevention Unit Series Paper 68, Home Office; *Towards a Safer Sutton? Impact of Closed Circuit Television on Sutton Town Centre*, M Bulos ed., 1994, London Borough of Sutton; *Towards a Safer Sutton? CCTV: One Year On*, M Bulos/D Grant eds., 1996, London Borough of Sutton; *Closed Circuit TV Surveillance and Crime Prevention in Brighton: Half yearly Report*, P Squires/L Measor, 1996, University of Brighton; *Closed Circuit TV Surveillance and Crime Prevention in Brighton: Follow Up Analysis*, P Squires/L Measor, 1997, University of Brighton.

³⁷ "Big Brother too much", *The Observer*, 10 March 1996.

³⁸ "Spy TV clamp urged after obscene calls", *Western Mail*, 7 June 1996.

23 October 1997]

[Continued]

DISCLOSURE OF CCTV FILM

30. There are no controls on the disclosure of CCTV film by operators to third parties. The extent of the potential intrusion of privacy which this represents is illustrated by a case in Brentwood. In 1995 Brentwood Borough Council's CCTV system recorded a man in the town centre who was attempting to commit suicide by cutting his wrists with a knife. An extract from the film, showing the man with the knife being led away by the police, was subsequently released to the media. The extract was broadcast on BBC1 and Anglia Television and published in a local newspaper without the man's knowledge or consent.³⁹ Extracts from CCTV are increasingly featuring in television programmes, often concerning crime prevention. In our view, disclosure of CCTV material to third parties could only be justified if it were reasonably necessary for the prevention or detection of crime. In the light of these concerns, there should be strict controls over the retention and destruction of, and access to, material recorded from CCTV.

TECHNOLOGICAL DEVELOPMENTS

31. As the available technology develops to enable increasingly sophisticated methods of image collection, storage and transmission, there is inevitably further potential for misuse and abuse of CCTV systems. We would therefore submit that this Committee should, having established so far as possible the anticipated capabilities of digital technology, ensure that any recommendations it makes as to the protection of civil liberties will provide safeguards which match technological advancements.

Q.7. Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?

32. Liberty believes that, in view of the potential for significant intrusions into the privacy of individuals and the current lack of effective and enforceable regulation of CCTV, there should be statutory controls on the placement and use of surveillance cameras and the release of information from them.

THE CURRENT LEGAL POSITION

33. There are at present no statutory, or other, controls on CCTV in the United Kingdom. As regards local authorities, section 163 of the Criminal Justice and Public Order Act 1994⁴⁰ confirmed that, in order to "promote the prevention of crime or the welfare of the victims of crime", they may provide "apparatus for recording visual images of events occurring on any land in their area". This, however, was a provision intended to remove any doubt about the powers available to Councils outside London to finance CCTV systems.⁴¹ The police are subject to Home Office Guidelines published in 1984⁴² concerning police surveillance operations generally. These Guidelines acknowledge the risk that the use of CCTV may amount to an "unwarrantable intrusion of privacy", but, as guidelines, they do not provide any enforceable rights to individuals.

34. In the absence of a right of privacy, the Government's commitment to incorporate the European Convention on Human Rights into domestic law⁴³ may provide an individual whose privacy is invaded by the use of CCTV cameras with an enforceable remedy. For example, Article 8(1) of the Convention provides that *everyone has the right to respect for his private and family life, his home and his correspondence*. Incorporation of the Convention will therefore establish a general right of privacy, as against public authorities, but it is not clear what the extent of such a right will be, nor the extent of any remedies.

35. The Data Protection Act 1984 will apply to the operators of CCTV systems which are capable of automatically processing personal data by reference to the data subject. Where the 1984 Act applies, the data subject will have subject access rights and will be protected by the non-disclosure rules, subject to wide-ranging exemptions.⁴⁴ Whilst the technology to enable CCTV systems automatically to process images is readily available, our understanding is that most systems currently in operation by local authorities and/or the police do not meet these criteria and therefore the 1984 Act does not apply.⁴⁵

³⁹ Liberty is currently representing the man in judicial review proceedings in the High Court which seek to challenge the lawfulness of the disclosure of the material by the Council.

⁴⁰ Section 163 came into force on 3 February 1995.

⁴¹ See 556 HL Official Report (5th series) col. 1794, 12 July 1994.

⁴² *Guidelines on the use of equipment in police surveillance operations*, Home Office, 1984. Insofar as these guidelines relate to intrusive surveillance involving entry on or interference with property, they have been superseded by the Police Act 1997. We understand that the Home Office is currently reviewing the Guidelines.

⁴³ A White Paper is expected imminently.

⁴⁴ For example, where disclosure or subject access would be likely to prejudice the prevention or detection of crime.

⁴⁵ In order to implement the EC Data Protection Directive (95/46/EC), the scope of the 1984 Act will be extended to cover non-automated data. However, the July 1997 White Paper suggested that the provisions relating to non-automated data will not be implemented for 12 years.

23 October 1997]

[Continued

36. Many local authorities have adopted voluntary codes of practice, and, in particular, the Local Government Information Unit code of practice, *A Watching Brief*⁴⁶, has been widely adopted. A number of these codes have contributed to the development of good practice. However, such codes rely on the vigilance and self-monitoring of the body concerned and ultimately fail to provide an effective means of redress for abuses since they are unenforceable in the courts.

THE NEED FOR NEW CONTROLS

37. We therefore consider that a powerful case is made for statutory regulation. During the passage through Parliament in 1994 of the Criminal Justice and Public Order Bill, Alun Michael MP (now Minister of State at the Home Office) tabled amendments to that Bill (drafted by Liberty and the Local Government Information Unit) which would have required the Secretary of State to publish regulations in respect of CCTV. It was proposed that the regulations should deal with the following:

- restrictions to prevent the surveillance of private residential premises without the consent of the majority of the occupiers of those premises;
- the provision for the display of notices to the public of the existence of CCTV systems;
- the selection, training and supervision of the operators of the apparatus;
- arrangements for the storage of, and access to, any recordings made;
- arrangements for access to the recordings by the subjects of those recordings; and
- arrangements for the destruction of the recordings.

38. We believe that statutory controls are needed in order to regulate the matters listed above, and that the scope of regulation should be regularly monitored so as to be in line with technological developments. Such regulation should provide for independent oversight, complaints procedures and the availability of sanctions for individuals to seek redress against operators or owners of CCTV systems.

Q8. *Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?*

39. So far as law enforcement officers are concerned, perhaps the most important matters which should be emphasised are proper treatment of the medium in which the image is stored and upholding the integrity of the audit trail. In relation to the courts, the two most important aspects are the extent to which judges, lawyers, magistrates and juries (as directed by judges) appreciate and understand the limitations and dangers of digital technology and the related issue of ensuring that the facilities available in court for the viewing of digital images are of sufficient quality so as not to detract from the quality of the image viewed.

Q9. *Is there the need for special measures to control the publication of modified images by the media?*

40. The only remedies currently available to an individual whose image has been published in the media are complaints to the Broadcasting Standards Commission, the Independent Television Commission and the Press Complaints Commission. For example, a complaint could be made to the Broadcasting Standards Commission to the effect that the publication of a modified image had unwarrantably infringed the complainant's privacy and/or that the complainant had received unjust or unfair treatment. These Commissions may require their findings to be published, but they have no powers to require a respondent to pay compensation to a successful complainant or to compel a respondent to take any particular action (such as to publish an apology).

41. Nevertheless, we believe that unwarranted publication in the media would be best prevented by imposing adequate controls on the operators of CCTV systems to prevent disclosure to third parties unless it is reasonably necessary for the prevention or detection of crime.

29 September 1997

“New Techniques and New Devices”—video evidence and the criminal courts

Philip Plowden, Michael Stockdale, David Elliott

(1997) *New Law Journal* Vol. 147 502–504

Evidence from video cameras is now common in the criminal courts. It arises in high profile cases, such as the recent collapsed trial of the Whitemoor escapees, but practitioners are just as likely to find it being used in the most minor shoplifting and public order matters. As CCTV cameras congregate on high buildings and

⁴⁶ Liberty was represented on the working group which contributed to the development of the code.

23 October 1997]

[Continued]

multistorey car parks, the law seems to have been quick to adopt this new technology, although many matters remain far from clear.

Most advocates would probably not object to the showing of a store surveillance camera tape, but on what basis is this evidence admissible and what limits are there as to its use? What, for example, is the position if the images were of poor quality but have been subsequently been enhanced? What if the prosecution wishes to provide still photographs from the video, or calls a police officer to provide a commentary whether to explain what is happening, or to confirm the identity of the person on the video? Can the prosecution replay the tape during a trial—can a jury take the tape into the jury room? Can the video be shown in slow motion to identify the individual blow or the details of a participant's features? Can defence advocates require the prosecution to provide the original video at court, and what steps should they be taking to ascertain the authenticity of the video evidence?

This short article aims to identify some of the most pressing issues that arise from the use of video evidence in criminal courts.

THE EVIDENTIAL STATUS OF PHOTOGRAPHIC/VIDEO EVIDENCE

It is ironic that the law is generally felt to be slow to react to new developments, when in the case of photographic and video technology the courts have from the start been eager to use a technology that appears to do away with the ambiguities and uncertainties of eye witness testimony. As early as 1864 a photograph was being accepted as evidence of the appearance of Mary Tolson's first husband. He was, according to prosecution witnesses, alive and serving in India at the time of her second, and thus bigamous, marriage. The photograph, the trial judge held, was admissible as a visible representation of the impression made on the minds of the witnesses. It was therefore "only another species of the evidence which persons give of identity when they speak merely from memory."⁴⁷ From the start, therefore, photographic evidence was accepted as a form of real evidence, a direct account of what was perceived at the time, rather than a form of hearsay.⁴⁸

By the time of *R v Maqsud Ali* in 1965 it was possible for the Court of Criminal Appeal, in considering the admissibility of tape recordings of the suspects' conversations⁴⁹ to state that "for many years now photographs have been admissible in evidence on proof that they are relevant to the issues in the case . . . the prints as seen represent situations that have been reproduced by means of mechanical and chemical devices." The court concluded that there was no distinction to be drawn between photographs and tape recordings, stating that it would be "wrong to deny to the law of evidence advantages to be gained by new techniques and new devices".

It therefore comes as no surprise to find the court in *Fowden and White*⁵⁰ confirming that there is no difference in principle between a video film and a photograph or tape recording. Taken alongside the principle that such evidence is real evidence, it therefore follows that where a witness has seen that video evidence, they are in the same position as an eye witness and can therefore give first-hand evidence as to what they have seen if, for example, the tape is lost or recorded over (as in *Taylor v Chief Constable of Cheshire*⁵¹), or where there has been a later identification of the suspect by a witness viewing the tape⁵².

IMPROVING THE EVIDENCE—AUTHENTICITY AND VIDEO EVIDENCE

Photographs are traditionally produced by the action of light on treated film, which is then further treated with chemicals to produce a negative image. Such negatives can be "retouched" to improve or alter an image, and the courts have dealt with this by requiring a statement from the photographer confirming that the photographs are taken from unretouched negatives. Digital images, however, are recorded as a stream of numeric values. Where there has been manipulation, it is hard to find physical traces of the changes. Authenticity as such is rarely in issue—in the sense that few lawyers find themselves arguing that the video image has been faked. What is more likely to be of concern—and challenges the idea of the photograph as a clear window through which the original event can be witnessed—is the enhancement of images.

Enhancement should never add to an image; it should merely expose information which is latent in the existing image. Clearly a copy of the original should always be kept, but with any copying process some information is lost, so that often it will be necessary to work with the original. Equally, where the original is on a tape, this may already have been viewed a number of times by the investigating officers. Where a tape

⁴⁷ *Regina v Tolson* (1864) 4 F&F 103.

⁴⁸ In *Cook* [1987] 1 QB 417, however, the court went further, stating that "the photograph, the sketch and the photofit are in a class of evidence of their own to which neither the rule against hearsay nor the rule against the admission of an earlier consistent statement applies." [p.425]

⁴⁹ *R v Maqsud Ali* [1966] 1 QB 688. To add to the complexity of the case the recordings were covert, of poor quality and the suspects were using a "slang Punjabi dialect".

⁵⁰ *R v Fowden and White* [1982] Crim. L.R. 588.

⁵¹ *Taylor v Chief Constable of Cheshire* [1987] 1 All ER.

⁵² *R v Grimer* [1982] Crim LR 674.

23 October 1997]

[Continued]

has been "paused", the tapeheads will continue to spin at about 1,300 rpm, thus physically damaging the image further.

Enhancement is rarely challenged, presumably because most lawyers lack the technical knowledge to do so. Our experience is where defence lawyers do raise questions, they tend to be at the superficial level: asking where cameras were mounted; asking how a final video image is retrieved from a multiplex tape, which will be recording a number of images from different views in quick succession. Since most enhancement will be done by first digitising the image, a certificate under s.69 PACE should always be provided since the information has been "produced" by a computer.

A good example of the danger of enhancement is in relation to car number plates. Here images may be "sharpened" vertically by programming the computer to take all black dots within given parameters of a black vertical and bring them into line. Thus where an image of a P has lost part of the curve, sharpening along the vertical could produce a 1. Sharpening a blurred P along the horizontal might produce an F, or turn a B into a P. This is not to imply misconduct, the enhancement process may legitimately produce a number of different results.

Where enhancement has been undertaken, there should be an "audit trail", with the computer logging each action⁵³. Again our experience is that these are rarely, if ever, requested. Moreover, differences in heat, light and equipment tolerances will often mean that a second technician following the same audit trail may nonetheless find it impossible to duplicate the original enhancement. What is critical, however, is that the defence have access to the audit in order to ascertain the reliability and fairness of the enhancement process.

It should be noted at this point that it is clear that the best evidence rule does not apply to video images (see *Kajala*⁵⁴). Equally, where an original image is so corrupted that, even with enhancement, the image is of very poor quality, there will be an argument that the evidence is so little probative that it is insufficiently relevant to be admissible.

USING THE EVIDENCE—VIDEOS IN COURT

And how can this evidence, whether original or enhanced, be used in court? If video evidence is "real evidence"—or, *per Cook*, in a category of its own—is it on the same footing as a still photograph which can may be exhibited and taken into the jury room? The analogy is not with, for example, children's evidence on video under s.32A Criminal Justice Act 1988 since that video evidence is deemed by the Act to be "direct oral testimony". In contrast CCTV video evidence is more akin to a tape-recorded interview, where the current procedural rules require that the tape be replayed in court rather than the jury room⁵⁵, but where there appears to have been no caselaw as to whether such evidence can be replayed during the trial. The only guiding principle therefore is that of fairness to the defendant. On the one hand it can be argued that given the persuasive quality of video—the tendency to believe that, having seen the video, we have witnessed the event itself—repeated viewings of the video might improperly displace the alternative evidence given by eye witnesses, who will only be giving their evidence once. As against this it could be argued that replaying the video a number of times is simply the equivalent of examining or cross-examining a witness at length and taking them over an incident a number of times.

What if the prosecution wishes to call a witness to identify a person from the video—or to provide an explanation to the court of what is being shown? Identification at least is straightforward. Subject to the authenticity of the tape, evidence from a witness who recognises the defendant on the video is no different to testimony from a by-stander who was present: *Grimer*⁵⁶. This is subject to the principle that the defence must be able to properly cross-examine that person—so that in *Fowden and White*, where the identifying witnesses were the store detective and police officer who had previously arrested one defendant, the conviction was quashed since the defence could not properly cross-examine without revealing the circumstances of the original acquaintance. The case is a valuable reminder that s.78 applications to exclude video evidence may often need to be made to avoid any adverse effect on the overall fairness of the proceedings.

What then of the *Turnbull* warning in such identification cases? Where a witness identifies the defendant from the video, *Turnbull* remains appropriate, and indeed must be applied to the camera (ie. its position, its opportunity for viewing what it depicts), to the recorded copy (quality, relevance, distance etc) and to the witness (quality of identification etc.)⁵⁷. In *Blenkinsop*⁵⁸ Evans LJ suggested that where the jury was being invited to make the identification for themselves, the jury must take into account whether the defendant's appearance has changed, but need not be addressed further on matters that were obvious from the

⁵³ Home Office Improve is the only Home Office approved enhancement software, although various commercial alternatives exist. Improve automatically produces an audit trail and it does not allow information to be added to an image.

⁵⁴ *Kajala v Noble* (1982) 75 Cr App R 149.

⁵⁵ *Riaz; R v Burke* (1992) 94 Cr App R 339, but even this is not an absolute rule: *Tonge* [1993] Crim LR 876.

⁵⁶ *Op cit* at note 6.

⁵⁷ See speech of McNeill J. in *Taylor*, *op cit* at note 5.

⁵⁸ *R v Blenkinsop* [1995] Cr App. R. 7.

23 October 1997]

[Continued]

photograph itself, such as its quality, whether it was close-up or at a distance⁵⁹. In such a case a full *Turnbull* direction was inappropriate since "the process of identifying a person from a photographic image is a commonplace and everyday event" and thus within the jury's experience. However, the court went on to state that in either case there was "a general and invariable requirement that the jury shall be warned of the risk of mistaken identification and of the need to exercise particular care in any identification which they make for themselves."⁶⁰

But if a prosecution witness can attend court and identify the defendant from a video, can he go further and commentate on the actions of the defendant as shown on the video? Here the law is clear but unattractive. Where the witness, because of "lengthy and studious application", has "special knowledge that the Court did not possess"⁶¹ he can be treated as an expert *ad hoc*. Thus in *Clare and Peach* the officer who had taken good quality colour pictures of football fans entering and leaving a stadium, and had then watched the poorer quality black and white videos of a violent and confused fracas some 40 times, was entitled to point out to the court not only the specific incidents, but was also able to identify who he thought was involved and to state that he thought these were the defendants. The rationale for this seems little more than that it would be impracticable to afford the jury the same time and facilities to make the comparison for themselves.

There are a number of telling objections to this approach. The previous caselaw on experts *ad hoc* derives from other jurisdictions and is less enthusiastic than Lord Taylor's judgement in *Clare and Peach* suggests. While the court in *Howe* stated that: "Economy, convenience and despatch would commend the admission of such a commentary."⁶² The court in that case also remarked that such commentary would be inappropriate with more straightforward films, and that "in general if any commentary is reasonably required by the nature of the pictures it should be kept to a minimum."⁶³ Moreover, there is, of course, considerable research to show the great extent to which people tend to believe that police officers have particularly reliable powers of observation because of training and experience.⁶⁴ The effect of such a commentary—with the officer telling the court what it is that they are seeing and who it is that is doing it—is going to be extremely difficult to displace. When faced with such a case the defence will wish to argue that, relying on *Howe*, such commentaries should be the exception rather than the rule. If a commentary is permitted, the defence will then presumably wish to consider calling a similar expert *ad hoc* to explain why the film does not show what is alleged.

VIDEO EVIDENCE AND HEARSAY

It is clear that the video footage itself is not a form of hearsay statement. However, statements made in the film will be subject to the normal principles of evidence. Thus the comments made in the heat of the moment (which are adduced to prove the truth of the contents of those comments, rather than merely the fact that they were made) may, for example, be admissible under the *res gestae* principle. In any event such comments will be statements made in a document for the purposes of sections 23 and 24 Criminal Justice Act 1988, since document is there defined to include photographs and films.

Much video footage has time and date information recorded onto it, and this may be central to the case. There is caselaw suggesting that such information, if recorded purely mechanically, may itself be real evidence: *Statute of Liberty*⁶⁵. Alternatively, if the information is hearsay, admissibility will be determined by section 23 or section 24 CJA 1988. In either instance, however, the reliability of the information must be carefully ascertained. The time recording mechanisms on most CCTV systems are notoriously prone to "slippage" and we would suggest that advocates should always require evidence as to who programmed this information into the system, what source they used for the time (their own watch, the local town clock, the speaking clock?) and how often the accuracy of this was checked⁶⁶.

CONCLUSION

Video footage offers a new source of evidence of considerable importance, but if its undoubted benefits are to be fully exploited the courts and the parties involved will need to appreciate the potential dangers of the evidence and the proper limitations that should be imposed upon it. By trying to identify the basis on which the evidence is said to be admissible, and summarising the available caselaw on procedural points, we have tried to provide a starting-point for practitioners. Photographic evidence has a long history, but many issues

⁵⁹ In line with Evans LJ's earlier ruling in *Downey* [1995] Cr App R 547, modifying the rule in *R v Dodson and Williams* [1984] 1 WLR 971, which had suggested a modified warning was "imperative".

⁶⁰ *Blenkinsop*, *op cit* at note 12, p. 12.

⁶¹ *R v Clare and Peach* [1995] 2 Cr App R 333, at 338, quoting from the New Zealand case of *R v Howe* [1982] 1 NZLR 618.

⁶² *Howe*, *ibid*, 627.

⁶³ *Ibid*, p. 628.

⁶⁴ For a detailed critique of this area see Munday, *Videotape Evidence and the Advent of the Expert Ad Hoc*, (1995) 159 JP 547.

⁶⁵ *The Statute of Liberty* [1968] 1 W.L.R. 739.

⁶⁶ It is now clear that a wrong timer on an intoximeter will not render evidence from the device inadmissible under s.68 PACE: see the recent House of Lords decision in *DPP v McKeown, Jones* 1997 *The Times* 21 February. As the time was irrelevant in this case, no attention was paid to whether the information as to the time would itself have been inadmissible hearsay.

23 October 1997]

[Continued

are still far from clear. They will only become clear if practitioners are alert to the need to challenge unfairnesses in the use of such evidence so as to ensure that the value of video evidence is balanced by appropriate safeguards.

Examination of Witnesses

MS MADELEINE COLVIN, MR PETER NOORLANDER, DR CLIVE NORRIS, Justice, MR PHILIP LEACH, MR PHILIP PLOWDEN and DR MICHAEL STOCKDALE, Liberty, called in and examined.

Chairman

1. Good morning, ladies and gentlemen. We are very pleased to see you here. I am sure you are aware of what our enquiry is about, digital images as evidence, and there are, I know, some particular parts of our enquiry which are of interest to you. I would like, if I could, to start with Ms Colvin and Mr Leach and ask if you would just introduce yourselves for the record and those who are accompanying you.

(*Ms Colvin*) Thank you. I am Legal Officer at Justice and accompanying me today to my right is Dr Clive Norris from the Centre of Criminology and Criminal Justice at Hull University and who is a specialist in CCTV; and to my left is the Legal Researcher for Justice, Mr Peter Noorlander.

(*Mr Leach*) I am Philip Leach and I am a solicitor and Legal Officer at Liberty and with me today to my immediate right is Philip Plowden who is a Solicitor and Principal Lecturer at the University of Northumbria at Newcastle and to his right is Dr Michael Stockdale who is Senior Lecturer at the same university.

2. Thank you very much. We have a number of questions for you but perhaps to start us off—and I leave it either to you, Ms Colvin, or you, Mr Leach, as to who would like to go first—you would just say a few opening remarks.

(*Ms Colvin*) As we put in our written submission, I think it is clear that we have taken up two aspects of the enquiry separately. The first is the question of guaranteeing the reliability of the admissibility of evidence of images. We propose that there should be changes in the regime of the proof of evidence and the use of security measures to authenticate the reliability of the evidence. The second aspect concerns the use of digital images for law enforcement purposes, particularly the use of CCTV images, and the possibilities and implications for the future of using automated facial recognition systems with CCTVs. We think that it is opportune to deal with these matters now, partly because it has benefits for the law enforcement agencies but also because as a human rights organisation, we are concerned about the dangers and implications that it has for individual rights.

(*Mr Leach*) Liberty has dealt with the two aspects that the Committee is looking at, the evidential questions and then the wider civil liberties questions. As to the evidential points, we have concentrated on the principle of the quality of images and the issues that that raises in this context: the difficulty of being able to test whether evidence has been tampered with or not; the particular problems that the new technology raises; and lawyers and judges being aware of the new technology. Our view is broadly that there is not a great deal of awareness of the uses to which digital technology can be put and the possibilities for the future. On the wider civil liberties

issues we have pointed out that surveillance is completely unregulated and we believe there is a need for regulation of a number of aspects: the training of camera operators; the use to which the evidence is put; the disclosure of tapes—a whole range of issues that have been covered by codes of practice, which have been widely adopted by local authorities, but which as a matter of law remain unregulated.

3. Thank you very much. Can I take you up on that particular point which you make of there not being a great deal of awareness in courts. What more do you think needs to be done or can you expand on what you mean by a lack of awareness.

(*Mr Plowden*) I wonder if I might take up this point. I think one's experience in court is primarily to do with the quality that digital video evidence makes available to the court in proving matters and obviously the courts are extremely enthusiastic in adopting this evidence because it is so highly probative of guilt or innocence in these situations. The concern I would suggest in using this evidence, notwithstanding the quality, the flip side of that is the ease of manipulation that accompanies digital technology and the consequent difficulty of detecting manipulation in digital images. I was speaking casually to a barrister only yesterday who is dealing with a trial in two days' time in which there is only video evidence. It is a public order offence. There are Section 9 statements from the camera operators to confirm what is being videoed and other than that the prosecution will simply be playing a video of the incident to the court and addressing them accordingly that on the basis of video evidence the case has been made out. I suggest that five or six years ago that would have been a wholly unthinkable situation so obviously the courts have moved very quickly in adopting the technology. The concern would be that in looking at the quality of the evidence they would not necessarily be aware of the dangers that accompany it in terms of the ease of manipulation.

4. On that ease of manipulation, about which I think we all have some understanding, there is of course the related issue of auditing and the custody and security of material from the time it is obtained to the time it appears before the court. Now there is a need for awareness too about those particular processes. What is your opinion about that part of the awareness in the courts?

(*Mr Plowden*) Again, having spoken informally to the video technicians with our local police force, I understand that in six years an audit trail has never even been requested by the defence. Indeed, when I have mentioned this to local barristers and solicitors the words "audit trail" do not mean anything to them, as I must confess they did not mean anything to me a year ago. So although approved software used by the police, and I should stress that this is only

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Chairman *contd.*]

a requirement for the police to use the Home Office Improve (and I understand that Improve 2 is coming into use) produces an audit trail, firstly, there is no awareness of the existence of this audit trail and, secondly, it would only make sense to another computer expert. It simply details what steps have been taken in enhancing and manipulating the images, so unless there is another expert there to try and follow the audit trail and to look at each point to see whether a different result is not equally possible then an audit trail by itself, even if the defence were aware of it, would mean relatively little. I suppose a more useful thing would be if it were possible to have a system so that the court could see the steps that a technician was taking in changing the image and improving its quality, in sharpening the letters on a number plate so that instead of showing a B they showed a P, and they showed an I instead of a 1. If the court were able to see those steps it would be in a much better position to judge the overall quality of the evidence and come to its conclusions about what weight it should place on that.

Lord Howie of Troon

5. Could I just ask one question, Chairman. Would not the same objection be taken to the second video?

(*Mr Plowden*) Yes, it could equally be taken to the second video. I suppose what I am saying is that although there must be concerns about fabrication and although an important safeguard in the courts against fabrication is always the proper testing of evidence by the parties concerned, and I do not think that currently happens with video evidence, there is, if you want, a more commonplace concern because fabrication at some point concerns a conspiracy to pervert the course of justice and obviously with video technology the way it is it requires a number of people to get together to conspire to do that. There is a more commonplace situation where a video person is asked to look at a tape of a motorway and the police officer says, "I am looking for a black Ford Sierra", and the technician isolates a grey Ford Sierra and it is a poor quality image, as these things tend to be, and the police officer says, "Could that be the black one?" and he would say, "If you enhance it this way", and sure enough he enhances it and it produces the required result. My concern is that there is no one currently able to say, unless a defence expert is called and follows the audit trail accurately to that point, "Hang on, you could equally correctly enhance in a different direction and produce a white Ford Sierra." So it is that lack of opportunity to test rather than necessarily to identify fabrication.

Lord Flowers

6. This goes right to the question that I wanted to ask so maybe I can ask it now. I was going to direct it to Justice rather than to Liberty but in view of what has just been said it would be useful if both sides were to answer it. In the Justice evidence in paragraph 3.4 you give two ground rules and they sound sensible enough in general terms. The first one says that the enhancement of a digital image should not add anything to the image; it should merely expose that

which is already latent in the image. How do you know what is latent in the image? All you have is a block of computer memory which you can, if you wish, convert into dots of various colours on the screen. There is no image, there is no latent image. I am not just arguing about words, I hope. It matters because this concept occurs throughout your evidence several times and you seem to be putting great reliance on this concept of the latency which is a concept arising from ordinary photography where you slosh liquids on something and what appears is the latent image. It is not like that in digital technology. I do not understand why you put such reliance on there being something you can call a latent image.

(*Mr Noorlander*) If I may answer that. What we were worried about is not really what Mr Plowden was talking about where you enhance images, we were worried about the much deeper aspect where you deliberately manipulate an image. What we were then worried about was how you can somehow ensure that the image produced in court is the image as originally taken. We went into the question of watermarking and the encryption schemes and several other technological schemes that may be applied to somehow protect the original image. What we try to point out in our paper is that such technologies really can never be completely tamper-proof. We see four problems arising there. If you do apply any watermarking scheme or encryption scheme or whatever, that would have to be applied directly within the camera where the image was going to be captured so you would need some sort of hardware within the camera to apply this watermark or to apply this encryption. However, camera and video camera manufacturers operate globally so you would want to arrive at a global standard. I would imagine a manufacturer like Kodak to be extremely reluctant to manufacture one thing for the British market and one for the American market, so there is a global standard that you have to arrive at. Thirdly, any standard that is arrived at would have to be tamper-proof really and from the evidence that we got from our technical experts, who are unfortunately unable to be here today, such tamper-proof technology is extremely difficult to design. There is a difference between tamper-resistant and tamper-proof. The tamper-resistant technology would be technology which is resistant to tampering to a certain extent. With cheap software you would not be able to crack that but if you turned your mind to it and had a certain expertise in these matters you would be able to crack it.

7. I do not want to interrupt you but this ground rule you give, I understand it if it is a general exhortation to people to behave themselves. I also understand it if by putting it this way you are making a case for watermarking or something equivalent to that. Is that what the ground rule is intended to imply because it does not imply anything else to me?

(*Mr Noorlander*) It does not. In essence what we advocate is a dual system where the technological requirement is there but that must be backed up by an audit trail, and the fact that you must be able to show this chain of custody.

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Lord Flowers *contd.*]

(*Ms Colvin*) If I could add that when we use the word "latent" it is definitely related to the security measures as well. Fundamentally, we are saying that you also have to relate it to the need for security measures to be used at the same time.

(*Mr Plowden*) I wonder if I might pick up on that point. I speak with some diffidence because I do not regard myself in any way as being a computer expert. However, the term "latent" was one which I adopted from the use of a police video technical support officer who informed me that under the Home Office Improve system it was only possible to remove information, it was not possible under Improve—and I am conscious I do not speak from first-hand experience—to add information, so it would be possible, for example, to remove darkness which might be shadows or a moustache on somebody's face, but it would not be possible if you wanted to add darkness. I do not know how well that actually stands up, but I put that forward to show what is possible under the Home Office system.

8. Is it possible to interchange two images like that?

(*Mr Plowden*) As to that, I am afraid I cannot say.

9. That would not be an extremely difficult thing to do!

(*Mr Noorlander*) It seems to me if you can do one thing you can do it in reverse equally easily. If you can add shadows you can remove them and vice versa.

Chairman] You have highlighted an important area for us to take on further. I move to Lord Tombs.

Lord Tombs

10. Chairman, I have two points. Firstly, I was a little concerned at the opening remarks by Liberty which seemed to be for me anyway too narrow. We had references to tampering, fabrication and conspiracy. All these things may happen but also the translation system may have its own in-built corruption which may not require intervention and we should not lose sight of that. Secondly, I was rather puzzled by the described difficulty of the court interpreting an audit trail and the requirement for an expert witness. I think that is the case but expert witnesses are required for all sorts of information, medical and otherwise. Again, how does it differ in this case?

(*Mr Plowden*) A common area where expert witnesses might be required at the moment, although the courts might say they lack the expertise themselves to begin to deal with the evidence, would be in DNA evidence, for example. However, such cases tend to be crown court cases and the most recent statistical information suggests that less than one cent of criminal matters now go to trial in the crown court. What I think is unique about the video evidence is that it crops up across the range of criminal offences from matters which are wholly trivial like littering the street, for example, motoring offences. What causes particular concern is that in the majority of minor matters dealt with in the magistrate's court no legal aid is going to be available at all and for better or for worse defendants will be representing themselves. Even in those matters where legal aid is available the fixed fee system as it operates

in the magistrate's court leaves comparatively little leeway for detailed work to be done on the case and if an expert were to be instructed to have a look at the video evidence that was being relied on in the matter authorisation would have to be sought from the Legal Aid Board and I do not imagine that most computer experts would be prepared to put in a day's work for less than £300 or £400 a day and I do not imagine that the Legal Aid Board—certainly in an area like our own, Newcastle, where video evidence is very common—or the Lord Chancellor is going to be best pleased to find a lot more extra money so that each piece of video evidence can be properly tested. Which is why I suppose I was suggesting that although experts would be the way forward I think with video evidence where the use is so widespread, it might not be as easy to find that expertise in court.

11. It is a practical matter of scale not principle.

(*Mr Plowden*) I think what is so interesting about this area is the way in which different areas of science and law and developments in technology do meet with the practical and what is happening in court which is why I cited the case going on purely on video evidence because that is now happening and I am not sure (certainly within our academic circles) that we are necessarily aware when we write our books on evidence and procedure that this is now evidence and procedure.

Baroness Hogg

12. This takes me exactly to the point that I wanted to come in on because I fully appreciate your point that if every magistrate's court case involved this type of exchange between "titans of the nerd world", the whole system would go into complete gridlock. What I was not therefore sure about was whether you were pointing us toward a system, I do not know whether you would categorise them, and the extent to which you can rely on them in relatively small cases. You were trying to use, as it were, the eye of the magistrate or the eye of the jury at a certain level to look at the original image and judge for themselves the extent to which they could rely on the assertion by the prosecution that this definitely was a black Sierra not a grey one or whether that is just so weak that something has to be built into the system. I am not quite sure what the second video is beyond "Here's the original and here's the one we are basing our case on."

(*Mr Plowden*) I very much take the point, my Lord Chairman. I think it is a matter of ensuring that the court is aware of that original image. But, as is now so often the case (it is less so with digital technology but obviously many of the cameras still work on analogue technology) the quality can be remarkably poor so that at that first stage when the court is looking at it there may be an argument as to whether this evidence is admissible at all on the basis that it is so poor that it is irrelevant. It is only once the enhancement process has begun to take place that the court could consider the evidence. There then comes a second danger which again none of us academics seem to pay very much attention to that as soon as this video image is being played within the court the court, whether it is the jury or the bench, is naturally

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Baroness Hogg *contd.*]

looking from the person in the dock to the video and back again for however long it is playing for, which if we lawyers were to do it in court would effectively be a dock identification and would not normally be permissible because of its very prejudicial effect. By the time the arguments as to the status of the video had finished the court would have an absolute subconscious certainty that this must be the same person because they have been invited to make that comparison for the last while.

Lord Brain

13. Baroness Hogg has to a certain extent made the point that I was going to make in that there is a need to show the original image and the stages of enhancement it has gone through. I think you may agree that this does involve a barrister being able to understand how enhancement works or how the computer programme side of it works because whether it is analogue or digital the process it goes through is digital and it is a matter perhaps of doing that. I have got another point about ensuring that the original is original but would you like to comment on that first?

(*Mr Plowden*) I wholly agree and I think what it goes to is the point that was perhaps made when we started off this morning, the question about what the court understands as to the quality of the evidence because to some extent the courts understand nothing, they are simply there, as it were, to hear what the barristers or solicitor advocates are putting to them about how to treat the quality of this evidence. So a greater degree of education among the legal community might well help that. I think that comes in time anyway. I note from seeing law reports that the courts and barristers seem much more ready to deal with disputes on DNA evidence and presumably this is a case of technology which people are becoming a little bit more familiar with so maybe that will work its way through, but I think the idea of taking stages from the audit trail so the court can actually see what was happening is a very valuable one.

14. On the question of origin and identification of origin many modern video systems record date, time and location automatically as part of the data. Do you feel that that is adequate or do you still wish to have watermarking because again if you trace it through the images perhaps half an hour before and half an hour after it will give you a degree of certainty as to whether or not that is correct. The other thing is there are such things as read only memories and if they are going to do an enhancement ought they to put on a read only memory disk of some form the original so that that can be genuinely shown in court?

(*Ms Colvin*) Certainly Justice would agree with you that there are a number of ways of using devices to ensure the security of the original image, how it was taken and to keep that as part of the audit trail. Whether it is using the date and time or some other watermarking is a question of degree, really. What we would also say is that every system used in evidence in court should have gone through that security process. It is not just about having experts in

court on both sides to look at the audit trail. It is necessary also to have systems of security which are part of the evidence. It is part and parcel of being able to admit that sort of evidence. Clearly you would then have to have some level of agreement as to the approved systems that are entitled to be used when the evidence is put into court.

Chairman] Thank you very much for that. Perhaps we could move on. My Lord Bishop?

The Lord Bishop of Leicester

15. It may be that we have covered this but for clarification could I take you back to the question of watermarking and encryption. What you are saying is that however technically sophisticated a system might be it is not foolproof and that it therefore must be backed up by another protection such as an audit trail. Is that the position that you are taking?

(*Mr Noorlander*) That is absolutely correct; it must be part and parcel of the audit trail.

16. That is not to say that watermarking and encryption is not a useful technique to use but it is not adequate by itself?

(*Mr Noorlander*) That is absolutely correct.

(*Mr Plowden*) The audit trail, of course, starts only at the point that the tape enters the authorised systems. The tapes come from all around the towns and localities. You are only therefore auditing what you are doing officially. There is no guarantee that the tape has not been tampered with in some form before it gets there. I am not saying that is a commonplace occurrence but I just make the point that there is that gap.

17. Even the two together do not give a foolproof system?

(*Mr Plowden*) I think my concern would be not that we were able to create a foolproof system but that we were able to create a system that people were able to supervise properly.

(*Mr Noorlander*) My Lord Chairman, if I may add to that. Any system will never be foolproof because there is the human factor. You cannot protect against the originator, the photographer lying in court. You can protect against that to a certain degree but not if he somehow has the technology to tamper with the image or manipulate the image to such an extent that it escapes the current security procedures and on top of that lies in court as to the authenticity of the image. That is a problem you even have with film-based photography.

Lord Howie of Troon

18. Mention was made earlier, my Lord Chairman, of a case coming up in a day or two in which the only evidence to be offered was video evidence. Is the suggestion that that is proper or should video evidence always be backed up by evidence of some other kind?

(*Mr Plowden*) This is the matter I was being questioned about to see if I thought that it was possible. I think the best answer is that we do not yet know because the law is developing so fast. It must be said that the courts are generally seen as being slow to

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Lord Howie of Troon *contd.*]

react to development but they have always been keen to adopt video technology although I do not think that the courts have quite worked out the basis on which they are accepting this evidence. There are technical arguments as to whether this is real evidence.

19. My question is do you think it is proper, not what the courts are doing.

(Mr Plowden) At a personal level it concerns me.

20. I am thinking of Liberty. Does Liberty think it is proper or does Justice think it is proper?

(Mr Leach) I think we would say it should be backed up by other evidence.

21. You are suggesting that video evidence only should never be permitted?

(Mr Leach) I think it is difficult to be categorical because it is such a developing field but I think it should be exceptional.

22. Does Justice agree?

(Ms Colvin) No, I do not think we would go that far. If the video evidence is of the quality and probity to be good evidence in itself, and there are the judges overseeing the admissibility of that evidence and the fact that it has to go through the sort of security regime we are talking about, it is as good as identification evidence.

Lord Howie of Troon] Thank you.

Baroness Hogg

23. I just wanted to press Mr Leach on what he was saying about being backed up with other evidence. I am not clear what you are saying. Should there be somebody to answer for the operation of that surveillance or shot or are you saying that there has got to be completely separate evidence from the video which would be quite different?

(Mr Leach) We would say that there should be someone able to explain the steps of how the video evidence was obtained, where the camera was positioned, when it was taken, that sort of very basic evidence.

24. So what you are saying is that it should be able to be relied on here provided there was someone who could answer for the system being used?

(Mr Plowden) Yes. It is certainly the case that there are standard Section 9 statements from the video operator to confirm the position of the camera because otherwise it would not be admissible and there should also technically be a statement under Section 69 of the Police and Criminal Evidence Act because a computer is being used, although the ambit of that is now limited. Beyond that, if you want substantive evidence before the court on what happened that night it appears to be purely video.

Lord Ackner

25. Is it not vital if you are going to have video evidence on its own or even video evidence which is attacked, that there is the appropriate warning given to the jury as to the potential dangers and the limitations and the odd results that do sometimes occur? If you give an adequate warning do you think

that will strengthen the position that the right answer will be achieved?

(Dr Stockdale) If I can take that one. I think one problem is that in the course of jury trials, judges' summing ups can be very complex in a long and complex case and that the relevant direction is one of a number of other directions. English law tends to be based on the presumption that if all the directions are correct and proper then the law has been followed and the decision of the jury is final but the problem is of course whether the jury actually understood the relevant direction in the context of a complex summing up and how does its weight in their minds compare with the compelling weight of the evidence which they have seen? The danger is really that the direction itself might be swamped by the effect of the images and the complexity of the overall summing up. This leads to the general area of how juries make decisions which is not restricted to this particular context.

26. You have got the direction given in all identification cases where the jury is told that very frequently people who are convinced are wrong and the judge highlighting the opportunity of this, that and the other. That is generally accepted as being satisfactory.

(Dr Stockdale) That is right and, equally, when the jury themselves watch the video and make their own identification, a warning to the same effect is also given. I agree totally that it is essential that juries are properly directed as to the dangers of such evidence and also as to the fact that they must be satisfied beyond reasonable doubt, in the context of the various pieces of evidence they are looking at, whether it is the accused on the video? All I am suggesting is that it may be that the directions that are given are not sufficiently strong to counterbalance the factors Phil was referring to. For example, if they see the accused in court and see a fuzzy video image, they may eventually persuade themselves that the person is the accused even though the evidence is not sufficiently cogent. My only concern is what effect do warnings have on the minds of jurors? I think that this is a more general question.

(Dr Norris) Can I add something to that which relates back to an earlier issue which is if you have this fuzzy image one of the things that will increasingly happen is digital manipulation of that image to enhance it so that it produces a recognisable image and I think we are all familiar with the pictures of the killers of Jamie Bulger and how they were digitally enhanced. I think this is where some of the crucial issues in the future are going to lie because identification will rest, I suspect, or contested identification will rest on the quality of a particular image and this is not about people manipulating the tape deliberately. It will be part of the actual process and it is about how those enhancement factors actually change the nature of the image, how they will make a nose sharper or eyes come down slightly and that is going to be a problem. The person in the dock will be there and you will have enhanced images and I do not understand the technicalities of how the pixels, the little dots, are actually manipulated and you move the little dots around to make pictures which means that you are moving away from that

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Lord Ackner *contd.*]

issue. I think it is important from the audit trail argument that one sees what the original image was and of course actually understands the nature of those forms of enhancement and precisely what the pattern goes through. It depends on the different packages that you use. I doubt they are standard. Some will be one thing and some will be another and then you really do need expert witnesses. As we have heard, in the magistrate's court that may not be available so I think there is an issue here.

Lord Phillips of Ellesmere

27. Is there some minimum standard set for the quality of surveillance cameras, the resolution attainable, and so on, which does very much influence what you are describing as the fuzzy images that one starts with?

(*Dr Norris*) There are increasingly desirable standards published by the industry themselves and if you want a particular image of a particular quality it is well-known what sort of camera you should have, but there is no nationally agreed and universally accepted standard and in Newcastle after the riot two years ago after the last Newcastle game of the season, 120 pictures were released in the *Evening Chronicle* and the pictures were of an appalling quality and people were being asked to ring into the local police station to say who these people were. I do not think many of those pictures would have stood up in court as evidence but the police's argument was that many people walked in off the street and gave themselves up, so they were effective but whether they would have been effective in court had they been contested is a very different matter.

28. Would you then think that there should be some agreed national minimum standard for these systems?

(*Dr Norris*) It would be something that would need to be considered and I know that part of the industry would certainly welcome an agreed standard.

Baroness Hogg

29. Of course they can sell more better quality products. Is the market not going to take the whole thing up a gear anyway?

(*Dr Norris*) Could you please say that again?

30. Is the market going to improve? Are we going to see a process of improvement of quality? If there is doubt about the stability of the evidence then the value that it provides in having a low grade system is clearly not very great. Costs are coming down in this world and the industry wants to sell the new product. Is not the whole system going to drive up the higher quality of product?

(*Dr Stockdale*) If I could step in here. I think that the problem is not always the quality of the system. If you have got a shop or a garage which has a system installed which is of good quality, one problem is that they do not get the heads cleaned and they do not put new tapes in so that after two or three years they have a system which was perhaps of good quality but which has not been properly maintained and looked after. That is particularly true of analogue systems.

What you get in practice is often analogue tapes which are taken to police headquarters and then enhanced. Thus, the problem is not really the quality of the system, it is the maintenance of the system. The police certainly find that a big problem when they receive outside tapes. The fact that, for example, the tapes have been used for two years and the heads have not been cleaned for two years is part of the problem. It is not necessarily the quality of the system itself.

(*Ms Colvin*) Can I just add there. Going back to this question of putting the security measures in at the beginning, you could insist that they comply with a certain standard if they are to be used for law enforcement purposes. We know there are a range of purposes for CCTV but you could put a bottom line for law enforcement purposes as part of the security system.

Lord Brain] Just because bad photos appear in newspapers it does not mean to say that the originals were bad: stills taken from a video tape are almost always of very poor quality. I just want to put that reservation on that piece of evidence

Lord Howie of Troon

31. Is there a British standard issued by the BSI?

(*Dr Norris*) I do not know. One would have to ask John Comfort that.

Lord Brain

32. If it is, it is out of date.

(*Dr Norris*) I did not bring my CCTV manual with me.

Chairman] That is a point to look at. Can we move on to question four. Lord Brain?

Lord Brain] I think really we have had that answered, unless you want to make further comments on the question which is the lack of equality between prosecution and defence. I thought we had explored that fairly well.

Chairman] Any more comments on that?

Lord Tombs

33. Could I ask a question which is very speculative, but then we have been dealing in speculative issues most of the morning. We heard earlier about the concern about whether legal aid would be available to verify an audit trail or not. It occurred to me to wonder whether the absence of legal aid might not automatically lead to dismissal if you could establish reasonable doubt during the course of the trial, or at least on appeal. If it is possible for the defendant to say "I am not being allowed to verify the quality"—

(*Ms Colvin*) If it is an evidential matter which they are unable to deal with without a lawyer, you return to the basic principles of a fair trial.

34. Right. Would that not tighten up the prosecution's reliance on such evidence—in time?

(*Ms Colvin*) In the longer term it may do but in the meantime I think there are people appearing to be heard before the courts now who would not

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Lord Tombs *contd.*]

necessarily know how to take that point without a lawyer and who possibly do not think it is of value particularly in the lower level of cases coming before the magistrates' court, for example.

35. That is the very difficult case of educating the legal profession, is it not?

(*Mr Plowden*) With respect, I think the legal profession would probably be only too pleased to help out on any number of cases, it is just I do not know whether the public would like to pay for a lawyer to be present in every case.

Baroness Hogg] I think it is educating the magistracy.

Chairman

36. We need to keep moving on. Could we turn to the question about whether surveillance systems reduce crime. Justice, I see, say that it is not a proven fact and others claim that it has certainly helped to reduce or deter crime. Perhaps I could ask our witnesses to comment on those propositions?

(*Dr Norris*) I am being asked to lead on this. I will start by saying I think the jury is still out and then I will explain why I think that. We have all been bombarded with news stories and television pictures which have been convinced that CCTV has reduced crime. It is quite interesting to note that I calculate that the public CCTV movement in the last five years has probably accounted for about £250 million of public money, over a quarter of a billion pounds. I tried to think today how much has been spent on evaluating that use of public money and I would have to put it at considerably less than £500,000, less than 0.02 per cent. CCTV was introduced by the last government before any evaluation had been properly conducted as to whether it actually reduced crime. There have only been four, maybe five, properly conducted evaluations by people who are statistically trained and criminologically aware as to the impact of CCTV. They have been conducted in Airdrie, Doncaster, Sutton, Brighton and Glasgow. The Glasgow study results are not available yet. What we have seen from those studies is mixed findings. The Airdrie study, which was perhaps the most positive, found a 21 per cent reduction in crime overall. However, in Doncaster the reduction was only six per cent. One issue that occurred there was there was major evidence of displacement to surrounding towns. In fact, most of the benefit was not gained wholly in the area under surveillance, it was gained in an area around where the cameras were, a so-called diffusion of benefits or halo effect. If we look at Brighton, Brighton experienced a ten per cent reduction although I spoke earlier this week to the evaluator of that, Peter Squires from the University of Brighton, and he said that one of the problems was that in the middle of the evaluation they changed the policing strategy of the town centre and put far more officers in a more sensible arrangement in terms of demand. There were far more officers on the street when there were a lot of people on the streets, they changed their shift system. He thought that perhaps half of that benefit could be accounted for by that change. In Sutton there was indeed a reduction. There was a reduction of 13 per cent in the area under

surveillance. However, in the borough as a whole there was a reduction of 29 per cent. So, in fact, there was less of a reduction gained in the area. This is one of the major problems there has been in terms of evaluating CCTV. CCTV was introduced in Britain starting from 1993/94 at the same time as we started to see a decline in the national crime rate. What has often been confused by many of the people who advocate CCTV—local police, local authorities and the industry—is the confusion between correlation and causation. They have taken them to be identical and they are not. We actually have mixed findings. CCTV seems to be effective used in conjunction with other measures in car parks at reducing car park crime in a limited area. As you move to bigger more disorganised space it actually becomes less successful at reducing crime. It is not very successful at reducing violent crime at all. In Brighton violent crime went up by one per cent at that time so it did not actually reduce it. Why is this? Most violent crime is drink related. Young men go to the pub, they drink too much, they come out and they fight. I think CCTV does almost nothing to change that sort of instinctive behaviour. It may help the police respond to the incident more effectively, it may be very good as a management tool which is why many people like it, but I think we will have to wait to see more results of properly conducted evaluations based on at least a couple of years' data both before and after. Many of the schemes that we have seen which have told that there are 50 or 60 per cent reductions have only looked at three months' data either side. We know that local crime patterns vary immensely. Unless you look at the trend data you cannot know the real impact of the scheme. The other problem generally has been that displacement has been almost entirely ignored. The two studies that looked at it very carefully were the Brighton and Doncaster studies. The Brighton study, for instance, found displacement from the streets into shops and pubs. Now, almost no police statistics actually talk about displacement because they do not have the sophistication to measure it.

37. Thank you very much.

(*Mr Leach*) Could I respond on behalf of Liberty? I find myself echoing very much what Clive Norris has just said so I will be brief. We would acknowledge that surveillance systems can assist in detecting and preventing crime and that is certainly a claim that many of those who operate the systems have made, that it has led to fewer incidents and increased rates of conviction. But we simply do not believe that there is adequate independent evidence to enable us to be sure about the extent to which crime has been reduced. As Clive Norris has already said not enough is known, for example, about displacement and not enough is known about the impact on different types of crime. As Clive Norris said, there may be a greater impact upon car crime than on crimes arising out of drug or alcohol use. Much of the research that I am aware of has focused on the short-term rather than the long-term. It is essential, in our view, that in considering surveillance systems any debate about the need for regulation has to be informed by the most accurate and up to date information that is available as to their effectiveness in reducing crime.

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Chairman *contd.*]

The reason for that is that if as a society we accept that a degree of intrusion into our private lives is an acceptable *quid pro quo* for improved crime prevention then, of course, we need to know how effective these systems are. At the same time, and this comes on to a later question, we believe that the general public are very largely quite unaware of the potential for intrusion into their private lives that surveillance represents both now and in the future.

Lord Howie of Troon

38. Turning from crime in general to more specific crime, is there any evidence relating to shoplifting?

(*Dr Norris*) There have not been many studies of the effectiveness of CCTV in private security. I have just read one which does suggest that there was some benefit internally but not nearly as much as one would expect. One of the problems in evaluating these things is it is actually very difficult to find out how much stock any shop actually has at any particular time to work out how much they have lost. It is a major task and it requires an awful lot of research effort to do. I think at a commonsense level it perhaps is a dangerous one to do. There are ways in which it may have some impact and one of the ways in shopping centres that I am aware of now is that the security staff are using CCTV to prevent people entering the malls. The people that they are barring are people who have shoplifted in one of the stores or who have in some way upset or brought themselves to the attention of the security guards. If you do manage to exclude all your known shoplifters that may indeed have some effect on how much gets shoplifted. It may actually not have much effect because you only go for the obvious shoplifters and not the successful professional ones.

Lord Flowers

39. You talk about the evaluators as if you have some confidence in them. I would like to know who these people actually are and why you have confidence in them, if you do? Is there an attempt to bring the evaluators together? It is a problem of statistical inference which is not a laughing matter. Do you bring these people together in a conference to decide a national strategy on how to evaluate the data that you have or do you just leave it to some enthusiasts in the local university to work it out by methods that you have no control over?

(*Dr Norris*) You ask who are the evaluators. One of the major evaluators has been Professor Jason Ditton from the University of Sheffield and the Scottish Centre for Criminology who has looked at Glasgow and Airdrie and has done a lot of work on evaluating crime prevention measures. In a sense I take your point. One of the things that happened at the last round of Home Office money that was given was that also included in the bid you had to make a statement to the Home Office of how you were going to evaluate the scheme. They made evaluation a component of applying for the bid. However, they specified no strategy for doing the evaluation, they specified no indication of how much of the budget, what percentage, should be used to do it, and indeed

I was approached by a number of forces who asked whether we could do it but of course on a shoestring "can we not use some of your students to help out?" When I pointed out that good quality evaluation took time and that people with professional expertise should be paid a fair consultancy rate people shrunk away very quickly because that was not seen as what their budget was to be used for.

40. Now you have said it I confess that is how I imagined it would be.

(*Dr Norris*) The studies that I was talking about are ones that have a degree of statistical competence to them and evaluative competence.

Baroness Hogg

41. My question follows on very neatly from that because I was also going to ask about the nature of these evaluations. I share your implied criticism about the way the government is much better at spending money than evaluating the way it spends it. I think one should want to see some candid evaluation by government. There is also the issue of the private sector's evaluation of security systems and that may have a quite different appraisal. After all if I am running a business what I want to discover is that it is getting people out of my shops. In a sense if I am displacing the shoplifters elsewhere then on my criteria that is a success, that is fine because I have got them out of my store, although obviously from a public policy point of view the criteria would be different, to try to reduce it overall or at least improve your management of the crime problem. Nevertheless, it may be that the private sector is spending money more effectively on that first stage evaluation. Were any of these studies that you have access to carried out by major retail groups, for example?

(*Dr Norris*) I do not know.

42. My point is they may be spending money and evaluating it properly in the way that the public sector does not.

(*Dr Norris*) It is quite probable that they do. Indeed, in public systems one of the things that the challenge competition asked for was contribution from private finance, from local businesses. One of the ways it was sold, for instance in Glasgow, was that it would increase footfall in the stores in the city centre. If the city centre was seen as an attractive place to go and if people were less fearful it would increase footfall. It is almost impossible for evaluators to get that information because companies are very, very secretive about how they are doing relative to their town centre competitors. I know that has happened in one evaluation in recent times. Also, again CCTV occurred at a time when we were coming out of the recession so footfall was increasing to some degree because people did start to spend a little more although not that quickly. Again there is an evaluation problem with town centre schemes.

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Lord Tombs

43. Has there been enough public discussion on the question of surveillance systems? Mr Leach implied earlier that there is a marked lack of public awareness of the extent and desirability of it. If there is now, how do we encourage it? There does seem to be a large degree of public acceptance of these, perhaps passive acceptance. What would you like to see happen?

(*Dr Norris*) The first thing is that there clearly is on one level a widespread public support in the way that you can see measured in the various attitude surveys from the Home Office. I have just read one done by the University of Cambridge as well which supports that. I will say one thing about this, that it actually depends very much on how you phrase the question. In fact, Jason Ditton from the Scottish Centre for Criminology has actually tested this. If you frame the questions in relation to concerns about crime and fear of crime and ask whether people accept CCTV you will get between 70 and 95 per cent support, somewhere around there. If you ask the same questions but frame them in a civil liberties context you will actually reduce that quite considerably, you could probably reduce it to less than 50 per cent. He has actually empirically demonstrated this in a recent paper. One of the questions is about how people think about CCTV, what frame of reference they put it in, but also what do they know about CCTV. The public really has very little idea of (1) how the technology is moving and (2) how systems are actually run and what they actually do. They have the image of a friendly person sitting there watching everybody going around as a vaguely protective way of catching criminals but the reality is rather different. Also they have very little idea that, for instance, in the City of London now if you drive into the City of London your car number plate is automatically read digitally and checked against the police computer. The Metropolitan Police are now going to do the same thing across the Metropolitan area. It would appear that more and more police forces are going to take this technology up. So there could soon be in a sense a national database of the movements of our cars and where we go in them. That is not how most people think about CCTV, nor do they think about CCTV as having the potential to automatically identify someone who has a shoplifting conviction and effectively bar them from every single shop in a town centre or a shopping mall. One can understand that one might be barred from one shop, the one for which one has been convicted, but that creates a major extension of the consequences of a criminal action. That may be a very good thing, one may argue that that may reduce crime immensely, but it also raises major issues of civil liberties about how far you can exclude people from a whole range of services and goods. These things are happening now, not digitally but they are happening in private security malls and in shopping centres on local estates and so forth. If the public starts to have that image I think you would find maybe a rather different debate. I read through the evidence of the Local Government Information Unit to this Committee before I came and I think the really strong point that came out there was the example of Tianamen Square. The Tianamen Square surveillance system was sold by Plessey as a traffic

management scheme but once you have the technology it can be used for all sorts of reasons. What separates a democracy from a dictatorship is the forms of accountability and the forms of political control that we exercise over these forms of technologies.

Lord Tombs] My Lord Chairman, I would find it very helpful if we could have a reference to the two attitude surveys that Dr Norris mentioned, the one with a law enforcement bias and the other with a civil rights bias in the question. That happens all the time.

Chairman] If you could let us have that after that would be helpful.

Lord Tombs

44. This intrusion of data transfer is all pervasive, credit ratings and so on that pass between agencies. Presumably the Data Protection Act should have a role here, certainly as far as the exchange of information between surveillance authorities goes. Would you like to see that tightened or extended?

(*Ms Colvin*) The Data Protection Act has a role to play on CCTV but at the present stage it is quite limited. It really does depend on the way that the matter is recorded and how it identifies an individual. What it does not cover is a system of data matching where the image of identified individuals identified is stored and matched against another database. This is where the Data Protection Act cannot effectively bite. Data matching is not covered under the Act other than on a case by case basis. It does not cover the wide range data matching. It was an issue that Justice looked at in quite a lot of detail when the Social Security Fraud Bill was in Parliament about a year ago. It was actually the first piece of legislation trying to tackle data matching. Although the practice had been going on between government departments it was not that legal until it had a sound legal base to it. We looked comparatively at a number of other countries where it was significant that public discussion about data matching had been very broad, very wide, and had resulted in controls that were specifically identified as dealing with data matching. In Australia and New Zealand there is legislation and statutory codes of practice dealing with different sectors of data matching. That is what we are now proposing. We have now got to go down that route, we cannot leave it to a broad Data Protection Act, We have got to deal with data matching on its own as an issue for data protection which is extremely significant.

(*Mr Leach*) Can I make a number of points to bring it all together? The Data Protection Act dates from 1984 and it was not written with current technology in mind. It has a number of problems in that its exemptions in relation to subject access and non-disclosure are too wide. I would agree with your suggestion that it needs to be looked at. The Registrar's powers are too limited. Also there is the question of the Registrar's resources. We do not believe that the Registrar has enough resources even now to deal with all the powers that she has. I would like to return to the point about how we go forward. One way, subject to cost of course, may be a fully researched Home Office or Law Commission consultation process. If that happens, as we have said, the public need to know its effectiveness in

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Lord Tombs *contd.*]

reducing crime and the public need to be clear about the concerns that groups such as Justice and Liberty have expressed. It needs to be very, very wide consultation. It should go to community groups, people who have concerns about street crime, it needs to go as far as it can. It needs to deal also with the question of residential schemes, on which, as far as I am aware, there has been relatively little work. We did not see why such a process would cause the concern that the question implies. It would allay the fears that we know the public do have from the surveys that there have been. It would inform the public and it would demonstrate that measures were being taken to deal with those concerns.

Chairman

45. Could I take this question one step further and ask if the European Convention on Human Rights were to be incorporated into United Kingdom law would that resolve these civil liberties issues in your mind as far as CCTV and surveillance is concerned?

(*Mr Leach*) I understand that there is a Bill and a White Paper due to be published tomorrow on that. Some of the questions that will be raised will depend on the way incorporation is carried out, but in general it will establish a right of privacy. Article 8 is the right to respect for your private and family life, your home and your correspondence. There is, however, no question that intrusive surveillance of this sort will come into Article 8. There is a body of case law on Article 8 in Strasbourg. There is not much, I have to say, on visual surveillance, on the question of cameras. There is, however, a lot of law on surveillance in terms of telephone tapping by the state (by the police and by the security services). What the Strasbourg Commission and Court have said in general is that because surveillance can be so intrusive the law must be very, very clear and very, very precise about circumstances in which surveillance can take place. I think that is the point I would stress. It would create a general right of privacy and then it would be up to the courts here to evaluate the previous Strasbourg case law in working out how that would apply here. The Bill would certainly relate to public authorities. The more difficult question is whether it would deal with surveillance by private organisations. That will depend partly on what the Bill says tomorrow.

(*Ms Colvin*) There have been very strong arguments to say that CCTV as it is now is in breach of Article 8 because it is not in accordance with any law. If you invade a person's privacy then it has to be in accordance with the law. That has been strongly argued by lawyers. It has not actually been tested but that is likely to be so when you have got incorporated conventions.

Chairman] Thank you for that. Can we move on now to question seven. Lord Nathan?

Lord Nathan

46. I think we have to ignore the point that you have raised in answer to my next question. Do you see the need for specific legislation to control surveillance, perhaps that includes the custom and

use of the material, in all public spaces or only publicly owned spaces? Do you see it in private spaces which are open to the public, and that includes shopping? It is not only the big shops, the Marks & Spencers and the banks, but also the small shops. Would strengthening the legal status of the code be sufficient for the purpose or do you think there is a need for a separate national body to certify installations and then, of course, comes the question as to how you enforce this? That is a big question, I am sorry.

(*Mr Leach*) On the first point about public space, we believe that surveillance in respect of all public space should be controlled. It would be quite arbitrary if surveillance of public space which was in fact privately owned was left unregulated. To give you one example: we believe there should be no distinction between a town centre shopping mall owned by a local authority and a mall which in fact has been leased by the local authority to a private company. In both cases the extent of the public's access will be the same. It is the reality of the access and the use of the space which should determine the need for regulation rather than the question of who is technically the owner of the land. I raise one example here: Liberty is currently acting in the European Commission of Human Rights for ten young black men who were excluded indefinitely from their town centre. It had been leased by the local authority to a private company. In that case, which is going through the Commission at the moment, we say the fact that the centre is privately owned should make no difference to the extent of the rights of the users of that centre because there is public access to it. If your question is going on to within shops themselves then I think that is more difficult.

47. That is the interesting point. I went into a very large insurance broker's office the other day and I found CCTV in the entrance. It did not worry me but it occurred to me in the light of this enquiry to be a question I would put to you.

(*Mr Leach*) I think it raises very difficult questions. The systems will be very different. If you think of a newsagent with one camera and one television screen, that is very, very different from, say, the Newcastle town centre scheme. Clearly questions of, say, staff training will be very different. However a number of the principles that are in the Local Government Information Unit Code should equally apply, such as disclosure of the tapes. I am not sure whether there should be any difference in principle about when and in what circumstances tapes should be disclosed outside that system. Going on to your second point about the Local Government Information Unit code of practice, we certainly support it as establishing some very, very important principles and standards. It was drafted as a voluntary code, it was not drafted as something which was intended to be given legal status. I think each provision would have to be looked at very, very closely. It is an excellent starting point. It would be useful to review the effectiveness of the code itself and I understand that is work that the Unit is intending to do. It would be important to consider the technological developments that there have been since the code was researched and written in 1995 or

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Lord Nathan *contd.*]

1996. The last question on the need for a separate national body to certify installations, again we would support that. There is a need for an independent certification system to ensure compliance with any relevant statutory regulations, not only when surveillance schemes are set up but at regular intervals thereafter. That is a role that it has been suggested could be taken up by the Data Protection Registrar. This will depend on the extent to which the technology of those surveillance schemes allows automatic processing and therefore whether the Data Protection Act will apply or not. If that were to happen, as I said earlier, the Registrar will need a lot more resources.

48. I have one marginal point. Why do you draw a distinction between Marks & Spencer, just as an example, and the local newsagent so far as the installation and the use of CCTV is concerned?

(Mr Leach) I would not necessarily draw a distinction between shops, I would draw a distinction between a privately owned shop and a street or a mall which has public access to it.

49. So you would draw a distinction between a mall and the inside of Marks & Spencer?

(Mr Leach) Yes.

50. But you would not draw a distinction between Marks & Spencer and the local newsagent?

(Mr Leach) That raises a very difficult question. I think I would. In the case we are involved in in the European Commission the mall previously was a crossroads of public highways. The need for regulation of that public space is greater. I am not saying there should not be regulation of systems in private shops. I do not have the answers. It is a very difficult question.

51. You are reserving your position on that.

(Ms Colvin) I think you have to go back to principles and why there is a need for regulations, particularly if you look at Article 8. The fact is that you need a basis in law to safeguard against privacy invasion which is deemed to be necessary in a democratic society. That privacy invasion is going to take place whether it is in a public space or whether it is in a place such as Marks & Spencer which is being used in a public sense. Obviously it is a question of degree. At the end of the day the privacy safeguards are about what is going to be done with the data that is collected and the use of it. In that sense it could be said that you are dealing with very similar situations whether it is a public place or whether it is a place that is owned privately but people have public access to it. We go back to the question of the controls based on the principle of privacy and based on the need to safeguard and, therefore, I do not think at the end of the day there is going to be a great distinction between the two in placing them under some control. The degree of controls may well be different. The statutory codes of practice may well be different for what you do in a public place and what you do in Marks & Spencer. Overall the principle of privacy means that there needs to be some control of both.

Lord Howie of Troon] I wonder could we be provided with a copy of Article 8?

Chairman] I am sure we could find that.

Baroness Hogg

52. You have answered half the question that I was going to ask but you have given me further worries because I can quite see that the system of regulation governing the use of such images if they were due to be brought for a court case would be important but I am slightly worried that a massive regulatory system would impose a huge cost on the small local newsagent because that seems to me further to reduce their advantage relative to the big stores that could perhaps cope with a massive new regulatory system. Nor is it quite clear to me what the essence of the invasion of privacy is in the actual setting up of the system. I quite see that there is at least potentially one in the use of the images but is it, in fact, any different from the issues that arise in the taking of a photograph of someone and selling it to the local newspaper? What is the essence of the difference?

(Ms Colvin) The privacy issue bites when you have got the data. There is an argument though, and it is coming through in some of the cases going before the European Court, which is this question of "do you have a private life in public space?" Even just the taking of the image itself, is that going to have some kind of chilling effect on exercising your other rights? Put in the context of demonstrations which has been an example. If you take video film or photographs of somebody in a demonstration, and then process it that and have it on a database you may well be causing some sort of chilling effect. Although that person is in public and exercising a right in public, there may be a right of privacy even in that context.

53. It seems to me that there are two strands of arguments going in opposite directions here. In relation to the argument about right of privacy in relation to the first example it is argued that you do not have that right of privacy not to be photographed or reported by the press for what you do in a public space.

(Ms Colvin) It is what they do with that photograph, is it not?

54. But there is a strand of the argument that says what you do in a public space should be less protected than what you do in your own home. In this argument we seem to be going in almost the opposite direction of saying there should be much more regulation of this system in public spaces than in private. I am not quite sure how these two principles can work.

(Mr Leach) Perhaps one answer to that is to come back to the question of what use is made of the images. Take the example of an image being taken by a public authority CCTV system and then being disclosed to the media. We say that of course images must and should be used for the prevention and detection of crime. That is what these systems are being set up for and that is what they are being used for, but when the image, say, of a distressed person is sent to the media, apparently on the basis that it shows the effectiveness of CCTV systems generally, that is unacceptable and is a very clear invasion of someone's privacy. I do not think that that principle should be applied differently to a newsagent's shop than to the Newcastle City centre scheme. In both cases we would say that regulations should stop, in

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Baroness Hogg *contd.*]

this example, provision of that tape to the media; it should only be used for the prevention and detection of crime.

(*Ms Colvin*) I think one would be surprised at what is considered to be a public place. For example, in France they have got a new law on CCTV so that no camera publicly outside of a building is allowed to look into any private space. That makes it absolutely clear that that is private space, a private residence. What we are talking about here is this sort of semi-public space, a shop is privately owned but it is basically used as if it is a public space. You go into a shop, you do not actually have to have consent physically to enter, although we are seeing this happening in some places. I think that is the distinction that we are trying to get to. If you are going into a place which you use publicly then there is no distinction between that and a very public place owned publicly.

Baroness Hogg] My point still is that while one strand of the argument relates in principle to the more you are in a public place the less protection you are entitled to because you should know that if you are in a public place, as we have heard in earlier hearings, if you are going to behave like x you are going to be photographed, the other strand of this argument seems to be more regulation on the use of public spaces. There is a conflict here, is there not?

Lord Flowers

55. Would that not include churches and hospitals and places like that which are also used by the public?

(*Ms Colvin*) Absolutely.

56. That is why they should be treated privately.

(*Mr Plowden*) If I might just briefly pick up on a point about hospitals. I do understand from contacts that hidden CCTV systems are frequently used now within areas of hospitals, particularly with a view to discovering child abuse cases with the rise particularly of things like Münchhausen's Syndrome. I have no hard evidence to back this up but I had a phone call from a journalist in Wales who said that his local hospital was using this frequently.

Lord Ackner

57. A very small point. So far as private property is concerned, if there is an announcement on the outside of private property saying "we use CCTV", is that not an answer to any suggestion that there should be something?

(*Ms Colvin*) I think it goes a long way. When we talk about controls we are talking about a range and degree of controls. That is one that has been clearly identified as necessary, that people actually know what to expect within that situation.

58. And therefore they cannot complain.

(*Ms Colvin*) No, but you still need the control in terms how of the data is used. You do need those data protection controls because, for example, you could still have police using the film from a local newsagents to data match with something else.

The Lord Bishop of Leicester

59. This is a related point about the question of hidden cameras that Liberty make in their submission. As cameras become smaller, more mobile, battery driven, etc., I am told that as a result of some of the school surveillance systems, for example in my own system, vandalism and petty crime has been reduced dramatically by the use of hidden cameras and moving them around so that nobody knows where they are. There is a warning outside that there is such a system but it is the very nature of the hidden cameras that has solved this particular problem. I wonder whether you feel your negative reaction to hidden cameras is always justified?

(*Mr Leach*) I think it is a question of balance. We do say that in principle there should be notices so that people are aware. That is a point that is made in the Local Government Information Unit's code. They say, for example, do not use dummy cameras so that the public are aware. It is a balance. Cameras can be placed high on buildings where they are often not seen and they cannot be vandalised but it is a question of balance. We believe that there should be public notification in the way that Lord Ackner has suggested.

Chairman] Finally data matching, which I think we have already touched on.

Baroness Hogg

60. I think we have reached the point where we all feel we need to know more about the applications of surveillance systems. I am not quite sure whether what we are talking about here is a problem of scale. For example, when we are talking about the ring of steel and the accumulation of evidence on the movement of cars, if it was simply a policeman coming along and taking the number plate down by the side of the street and checking it, do any of us think that there is an issue because that is what number plates are for after all. Is it simply the mass of accumulation and ability to profile somebody's life out of their car number plate with which we are concerned or is it the matching of that database against, I do not know, financial information in which case different sets of rules would apply?

(*Ms Colvin*) It is the data matching against huge databases. We put in our evidence the fact that we are going to have a digital database of everyone's driving licence photo and their passport photo. We are therefore going to have data for facial recognition possibilities. It is the extent to which if you do not have any controls then we do not know how far it can be used and how far, for example, you could use it for law enforcement purposes for targeting, for example, that is possibly not justified. I think it is about saying that there needs to be a debate now before it is actually put into effect. We have got systems that are on the lower level like car recognition number plate systems, we have not yet got a wholesale facial recognition system but let us talk about it now before it really does occur. Part of that is also to put into place not only the training that is needed and the safeguards but also whether there needs to be security built into any of the technology itself.

23 October 1997]

MS MADELEINE COLVIN, MR PETER NOORLANDER,
DR CLIVE NORRIS, MR PHILIP LEACH,
MR PHILIP PLOWDEN AND DR MICHAEL STOCKDALE

[Continued]

Baroness Hogg *contd.*]

61. Really the thought that an Audit Commission might do the trick is not enough?

(*Ms Colvin*) Not enough. You really have got to look at each sector of data matching and provide statutory codes for each sector. That was the experience in Australia and New Zealand particularly.

Lord Brain

62. Could I make one very quick point. Is not the point the speed at which it can be done and the fact that it can be done totally automatically without human intervention?

(*Ms Colvin*) Yes.

Chairman

63. I am afraid I am watching the clock. I was going to give you all a chance to make any final points as we have reached the end of our questions, or if there is anything that occurs to you subsequently we will be very happy to hear it. May I offer you the floor for the moment if you do want to make a point?

(*Mr Leach*) My Lord, might I just add three very quick points on data matching. Liberty did some work in relation to the Social Security Administration Fraud Act which will allow data matching in relation to the investigation of fraud. The three points of principle that we made in relation to that data matching concept were these: firstly, there should only be disclosure if it is reasonably necessary for the investigation of crime or some other strong public interest ground; secondly, there should be a clear procedure and there should be reasons in each case; lastly, there should be some independent oversight.

Chairman] Fine, thank you. Does anybody else want to make any final comment to the Committee? Can I conclude by thanking you all very much indeed, not only for your patience and your thoroughness in answering our questions but also for the work put into the written evidence which you provided us with, all of which has been most helpful. Thank you very much indeed.

Memorandum by Mr Simon Davies

I am grateful for the opportunity to present evidence to the Committee today. The subject of your enquiry is timely and important.

By way of introduction, I am a specialist in the field of privacy and data protection, and have worked for 10 years in a variety of environments assessing the impact of surveillance technology on human rights and on society. I hold two academic appointments related to this work. One is with the Computer Security Research Centre of the London School of Economics, where I am Visiting Fellow, and the other is with the Department of Law in the University of Essex, where I am also a Visiting Fellow.

I am also the Director General of Privacy International, a non-government organisation which was formed in 1990 to monitor and campaign on issues related to surveillance by governments and the private sector. Privacy International has strong views on visual surveillance, and I will come to these a little later.

Other witnesses here are much better equipped than I to address the issue of digital images used for the purpose of evidence. I propose to deal with points six, seven and eight of the Call for Evidence. Namely, the broader issue of use of the technology.

This Committee will understand that in recent years, the use of CCTV in the UK has grown to unprecedented levels. Between 150 and 300 million pounds per year is now spent on a surveillance industry involving an estimated 200,000 cameras monitoring public spaces. Most towns and cities are moving to CCTV surveillance of public areas, housing estates, car parks and public facilities. Growth in the market is estimated at 15 to 20 per cent annually.

Many Central Business Districts in Britain are now covered by surveillance camera systems involving a linked system of cameras with full pan, tilt, zoom and infrared capacity. Their use on private property is also becoming popular. Increasingly, police and local councils are placing camera systems into housing estates and red light districts. Residents Associations are independently organising their own surveillance initiatives. Tens of thousands of cameras operate in public places; in phone booths, vending machines, buses, trains, taxis, alongside motorways and inside Automatic Teller Machines.

These systems involve sophisticated technology. Features include night vision, computer assisted operation, and motion detection facilities which allows the operator to instruct the system to go on red alert when anything moves in view of the cameras. Camera systems increasingly employ bullet-proof casing, and automated self defence mechanisms. The clarity of the pictures is usually excellent, with many systems being able to read a cigarette packet at 100 metres. The systems can often work in pitch blackness, bringing images up to daylight level.

The technology will ultimately converge with sophisticated software programmes that are capable of automated recognition of faces, crowd behaviour analysis, and (in certain environments) intimate scanning of the area between skin surface and clothes. The power and capabilities of cameras will continually increase,

*23 October 1997]**[Continued]*

while the cost and size will decrease. It is reasonable to assume that covert visual surveillance will in some environments be ubiquitous.

The CCTV trend is not confined to Britain. Sweden—once pathologically opposed to such surveillance—is considering relaxing its privacy laws to permit public surveillance, while CCTV activity in Norway has prompted specific inclusion of such surveillance in the Data Protection Act. Meanwhile, CCTV activity has grown markedly in North America and Australia.

In my role both as academic and as privacy advocate, I have taken an active interest in all aspects of CCTV. My assessment of the impact of this technology is predicated on the following conclusions.

First, I firmly believe the overall justification for the technology is specious, untested and is based largely on emotive grounds. Claims about the impact of CCTV on levels and patterns of crime are frequently exaggerated and simplistic. For example, crimes of passion, crimes involving drugs and alcohol, and actions by professional criminals are seldom prevented by the cameras. Generally speaking only minor “opportunistic” crime is diminished by the technology.

Second, the primary impact of the technology on human behaviour has more to do with public order than outright criminality. In practice most camera systems have been used principally to combat “anti-social behaviour”, including littering, urinating in parks, underage smoking, traffic violations, graffiti, fighting, obstruction, drunkenness, indecency, and evading meters in town parking lots. There is, of course, an argument that these are legitimate targets for the technology, but few members of the public associate CCTV with such misdemeanors.

Finally, I believe the technology has numerous deleterious facets that are under-reported. I have personally witnessed CCTV system operators routinely exercising their prejudices to discriminate against race, age, class or sexual preference. A recent report from the University of Hull supports this observation. Several high profile cases of abuse of the technology and of images has contributed to a decline in public support for the technology. CCTV is also a key factor in a range of important changes to police practices. These changes—including a shift from pro-active to reactive policing—have not been adequately researched or assessed.

In short, a situation is developing in which CCTV surveillance is so commonplace that fundamental changes are occurring in policing, human behaviour and interaction, community development policy and personal privacy.

I support Privacy International’s view that immediate restrictions and prohibitions are required for three categories of CCTV equipment.

Computerised Face Recognition (CFR) systems that have the capacity to automatically compare faces captured on CCTV, with a database of facial images. Several police and commercial organisations are developing this technology.

Audio, infra-red, high sensitivity equipment, and systems operating outside the visible light spectrum. These include Forward Looking Infra-red Radar (FLIR) systems able to detect activity behind walls, and infra-red systems able to detect activities in darkness.

Miniature and micro-engineered devices designed for covert surveillance. Around 125,000 of these devices are sold each year from UK surveillance equipment outlets.

Electronic visual surveillance is emerging as one of this century’s most profoundly important developments, and its implications need urgently to be debated. To this end, I would urge this committee to recommend the appointment of a mechanism to investigate the CCTV industry and to recommend appropriate safeguards and legislation.

Reforms that might be considered include:

Planning jurisdiction which has been removed from local authorities, should be returned to councils to re-establish some democratic mechanism in the development of wide-scale urban CCTV systems.

The scope of law should be expanded so that the Data Protection Registrar has some direct say in the establishment and running of systems.

Minimum standards of training and conditions for CCTV operators should be implemented.

A prohibition on the sale or transfer of images from the systems should be instituted.

Examination of Witness

MR SIMON DAVIES, Director General, Privacy International, called in and examined.

Chairman

64. Mr Simon Davies, good morning. Thank you very much for coming and also for the written evidence which you have already submitted. We have, as you know, a number of questions that we

would like to go through with you but before we do that is there anything you would like to say by way of introductory remarks?

(*Mr Davies*) Thank you, my Lord Chairman. I appreciate the opportunity to be here today. I should

23 October 1997]

MR SIMON DAVIES

[Continued

Chairman *contd.*]

clarify one or two points. I have a number of hats that I wear in the privacy realm, I have a number of academic appointments, but I am speaking here today I believe as Director of Privacy International. My views will not fundamentally change, it is just that I get the chance to use more adjectives! I think I have the honour of being the first person ever to write a critical article in the national press about CCTV. I did so five years ago in *The Independent*. I think I was a lone voice judging by the hostile mail which *The Independent* received. That shows how far we have come in the discussion in a short time. I will briefly summarise the written statement that you have received from me but I would like to also augment it. As I see it there are two ways we can look at this CCTV phenomenon in Britain. The first is that it is, if you like, the fifth utility delivering benefits and services to the community and that is the way it is portrayed generally by the market. The second way you can view it is as a surveillance infrastructure which delivers social control and creates a diminution of privacy. Those are the two extreme views. I naturally go to the view that what we are creating is a surveillance mechanism and that any attempt to create a fifth utility out of CCTV would lead us into very hot water in the future. Continually throughout this discussion we hear that there is a justification for the technology because the public support it. I would like to say a couple of things about that. First, I am not entirely convinced that the public overwhelmingly supports CCTV. The Home Office itself in its original surveys concluded that a large percentage, a significant percentage, of respondents changed their views if they were confronted with a variety of scenarios relating to the effect of the technology. For instance, if people received a cue at the beginning of the question "Do you support CCTV as a means of combatting major crime" overwhelmingly people would say "of course I do". If, however, you go further into the subject and you brief people on some of the implications, you prime them, for example, on the potential for surveillance, if you tell them about the power of the technology and inform them that this is military strength technology in an urban environment, you find progressively that support slides. Most of the voxpops conducted by newspapers recently have shown a slide down to about 60 per cent support. Even if you were to assume that there is overwhelming public support, even unanimous support, I do not think that that clears up the privacy question. We have very, very clear cut questions about the privacy implications of the technology and we always have right the way through the development of the systems. A point I should mention is that we are absolutely convinced that most CCTV systems contravene the first principle of the Data Protection Act, that is the principle that demands fair and lawful processing of information. On the basis of some academic studies, most notably the study by Clive Norris and his colleagues at the University of Hull, and my own observations you would have to conclude that there is endemic discrimination and harassment, often against young people and blacks. That in itself would contravene the first principle. What would also contravene the first principle is covert surveillance. This is

controversial I know but people do not look above their own eye line. If you ask people what a line of roofs look like in their own street they will not be able to tell you. Cameras are invisible to most people. It is not good just to say "we put up a sign saying you are under visual surveillance" if the cameras are not visible in people's normal movements. I would regard this as covert surveillance. I contend the first principle is breached in a wholesale way by these systems. It is something I hope to raise with the Data Protection Registrar later this month. Our concerns very, very briefly, some of them are already in the written statement: in the long-term, and this sounds hysterical I suppose, we are worried that CCTV will become part of the fabric of our environment to the extent where it becomes invisible, to the extent where you simply will not be able to tell at any given moment, even in semi-public areas, whether you are under surveillance and that ultimately leads to a form of social control. Surveillance technologies always become technologies of control, it is part of the nature of the technology. You have to keep that in mind in drafting your protections. We are very concerned about some of the technologies coming on stream. The new automatic recognition systems, face recognition systems, crowd movement systems, these need to be viewed in a different way from ordinary cameras that record images in daylight. We are dealing here with very sophisticated software. I did not hear all of the evidence before I arrived here but I understand that there are concerns also by other groups about the potential for data matching and the potential linkage with major data bases, that is something we share. As these images become digitised they will become automated and with automation you will find a whole range of privacy concerns emerging. I suppose what we would call for would be some form of prohibition on the use of a range of technologies, I have mentioned which ones in the written evidence, certainly those that employ sophisticated recognition and analysis software. The public are not aware of the power of those systems and until they are aware and there has been proper debate they should be prohibited. Certainly under the new Data Protection Law coming on stream soon there should be additional powers to the registrars but we believe there should be specific powers related to CCTV systems. Finally, the whole question of oversight needs to be dealt with because the current voluntary code seems to be lacking in a number of respects.

65. Thank you very much for that Mr Davies. I think it is fairly widely accepted that this country is quite well ahead on CCTV compared with other countries but you do mention in your written evidence that Norway and Sweden are relaxing their laws because previously they have taken a very tough stance about surveillance. I wonder whether you could comment on that and in fact, in spite of what you said, is there not an indication that they feel that some of the concerns you have been expressing may be misplaced?

A. Again I do not want to draw too close a connection between my own views, and those purportedly reflected in public opinion surveys. Certainly in countries such as the Netherlands there

23 October 1997]

MR SIMON DAVIES

[Continued]

Chairman *contd.*]

is an increased level of public acceptance as people get used to the technology. I am not sure though in Norway and Sweden, for example, the public support has not increased, to my knowledge. In Norway the penal code was amended but principally, as I understand it, that was for the purposes of CCTV images as evidence rather than the establishment of a surveillance grid over the major cities. My understanding, certainly from Privacy International's members in those countries, is the public support for the systems is still very, very limited.

Lord Ackner

66. You said public support is very limited but there is public support, is there not, to try and reduce the degree of anti social behaviour on housing estates and the like. Does this not provide some assistance on that scale?

A. I think the answer to that question depends on what sort of society you want to create. If you want a society which controls that sort of behaviour through surveillance then you have the perfect mechanism with CCTV. If you believe there are other more grass roots, more human measures which can be taken involving, for example, community schemes then you would have to reach the conclusion that CCTV is not the answer and in fact can create a whole raft of other problems with it. Deviant behaviour is something which I think you can deal with through alternative measures at the community level but one thing that has come through very clearly is that CCTV tends to be viewed as the single solution. I know the Home Office has been stressing this is not the case but take a look, for example, at the submissions made to local governments, overwhelmingly they say: "This is an answer which should be supported and supported to the tune of a substantial amount of the budget for crime prevention". I think, if you like, there is a displacement going on, CCTV is taking an overwhelming proportion of budgets for crime prevention, I am not talking about Metropolitan Police but just community schemes, Neighbourhood Watch schemes, for example. You will find CCTV is covering a lot of that ground without there being adequate research into the implications. I am not entirely sure that we are there yet in terms of whether CCTV actually works, the criminologists have got a mixed view of that, certainly.

Lord Flowers

67. I am a little puzzled by the line our witness is taking, my Lord Chairman, saying perhaps you should not use techniques until they have been accepted by the public. You said it in the context of CCTV but there have been many scientific techniques adopted by the police for dealing with criminal behaviour long before the public understood what was involved: the breathalyser, DNA finger printing. I very much doubt whether DNA finger printing has been accepted by the public in any meaningful sense but it is nowadays used regularly and far beyond the extent it was originally thought possible. I do not understand your starting

point which is that CCTV should not be used because it does not know the public has accepted it.

A. I think the whole question of public opinion is a side issue. Certainly from a human rights' perspective and a privacy perspective it is irrelevant whether the public supports the technology or not or whether it supports the method of policing. I agree there is a lot of forensic techniques which the public would have no knowledge of and if we left it up to public discussion they would take years to implement. I am not proposing that, what I am proposing is a more rigorous approach to CCTV. For example, for years chief constables have been allowed to get away with making a claim that CCTV reduces crime by 90 per cent, this is not the case. All of the criminological evidence contradicts that claim. Sure, CCTV does reduce crime but why is it necessary to arbitrarily make up statistics.

Baroness Hogg

68. But you think it does reduce crime?

A. It depends on your context. It reduces some opportunistic crime, for example people who are walking past a shop and see a coat on a rack, they make a decision they would like that coat, it is a spontaneous decision and the existence of a camera may influence them. As I understand it crimes of passion, premeditated crimes, crimes by professional criminals, those are not influenced by CCTV. We are dealing with a marginal pattern, with a very minor extent of crime.

69. Since you have studied, obviously, a number of countries may I ask in making both those assertions—(a) that it reduces certain types and (b) that it does not reduce others—what evidence you would like to point the Committee to?

A. I think the work of Jason Ditton is probably the best known in this country, the Scottish Centre for Criminology. Ditton has done some excellent criminological work on this and also in his bibliography he has summarised most of the international evidence. Ditton has concluded that the overall reduction in crime, according to fairly narrow criteria, is about 21 to 23 per cent overall but he does not include displaced crime in that figure. We do not know the extent to which a crime is displaced outside of the range of the camera or outside of the immediate area of the cameras' control, the camera's ambit, that is almost immeasurable. Ditton certainly did not try to measure it. We have a situation here where we have on the one hand a popular figure of 90 per cent promoted by the systems' manufacturers and the police and the criminological figure which is many, many times lower. I think overseas there is a similar understanding.

Lord Nathan

70. You say in the reforms that might be considered: "Minimum standards of training and conditions for CCTV operators should be implemented". Now it is quite clear that the operators must be trained or it must be instilled into them that they must not improperly use the material which they are photographing or taking images of

23 October 1997]

MR SIMON DAVIES

[Continued

Lord Nathan *contd.*]

but do you go beyond that and if so what is the extent of the point you are making?

A. I think I would be very confident in saying that the guidelines which are laid out for the conduct of the operation of the systems is routinely ignored. It is routinely ignored because it is drafted by people who do not have to sit in front of multiple screens for ten hours at a time and you find that what happens in a control room is an evolution of a certain pattern of behaviour. The guidelines are promoted very widely but in reality in that hot house, in the control room itself, you find a different set of disciplines, a different set of codes and practices emerges. Again I point to the work of Clive Norris, very very recently published, which concluded that the practices of operators was fundamentally different from what was set out in the code. That is just part of having a closed hot house environment. You find it is almost impossible to enforce consistent standards.

71. Perhaps you can say something concrete about that. Most of us are not knowledgeable—at least I speak for myself—on the subject. What is it which the operators are doing wrong or not complying with what you think is proper conduct?

A. I will give you two ends of the spectrum. The first is criminal behaviour. There was an operator in Mid Glamorgan—I do not know if you are familiar with this case—responsible for a control room who was prosecuted, I think it was early last year, on 300 specimen counts of obscenity. He would have one camera trained on a public phone box and when a woman he desired walked past, he would call the phone-box from the control room. He would zoom in on the woman who inevitably would pick up the phone, and then he would make an obscene suggestion. He would then watch in full glorious colour the woman's reactions. It was only when BT traced back to the control room that the man was prosecuted. There has been a number of prosecutions of that nature. At a more ordinary level perhaps but far more common is endemic discrimination and harassment of groups. For example, *The Independent* ran an article where they had uncovered a series of problems relating to the Liverpool system where the young people had been claiming that the camera operators had been harassing them, had been deliberately singling them out, following them around. These were people not particularly known to the operators or to the police but they were young and felt quite intimidated by this behaviour.

72. How did they know it was happening?

A. You can see the cameras. The cameras have a form of communication. The camera operator will nod the camera in one direction or the other. Young people know, they have a communication with the camera operator. Probably of all the groups of society, it is young people who know the cameras are there, I do not think many other groups in society know, they do not give the cameras a second thought. There is a communication between the operators and the young people, certainly. The operators make it known that they are watching the kids. The young people told *The Independent's* reporter that this was

ongoing harassment, and that was the way they viewed it. There has been a number of complaints to most councils from blacks, from ethnic groups, from women who claim they have been tracked also, routinely followed say from the station to their home. The councils would say that is the more benign end of the spectrum because those people are just being watched for society's good but you can turn it round and say that it is harassment.

73. I am sorry to prolong this but I want to know how they knew that this was happening. If they are prosecuted and this is produced in evidence then that is clear but how on earth does a woman know that she is being pursued by cameras or in fact black people know that they are being pursued by the cameras? How does it operate?

A. Most cameras have a physical movement—pan, tilt and zoom—so you can see where the camera is pointing. Once you are tuned to the existence of the cameras, once you are familiar with the cameras as part of your environment, you watch for them and you can see the angle. Let us say you have a friend and your friend alerts you to the possibility that you are being watched by the cameras, you will watch the angle. Some women are claiming that whenever they watch the cameras, the cameras are looking straight at them and even if they moved around as they walked down the street the camera was following them and they can see this. There have been numerous complaints and we have had complaints, where you direct the complaints is another question. We will be looking at the possibility shortly of urging prosecution under the stalking law, I do not know how far we will get with that. A number of women who have contacted us have complained that routinely the cameras will single them out and follow them.

Lord Nathan] Thank you very much.

Chairman

74. I think the clock is beginning to beat us Mr Davies. We did have a couple of other questions, one to do with the powers of the Data Protection Registrar. I wonder if you have any views on that and whether you would be kind enough to submit them in writing.

A. Yes.

75. Whether the various technologies which you have been talking about which you perceive should be restricted, whether that is better done by a code of practice, bearing in mind the difficulties of trying to legislate about particular technologies when the old field of technology is changing very rapidly. Could I put that to you and if you could respond to those two points I would be most grateful. I am sorry to have to cut it short here but we do thank you very much indeed for not only your written evidence but for your very clear and well presented points before us this morning. Thank you very much indeed.

A. Thank you.

THURSDAY 6 NOVEMBER 1997

Present:

Ackner, L.
Brain, L.
Carmichael of Kelvingrove, L.
Craig of Radley, L.
(Chairman)
Flowers, L.

Howie of Troon, L.
Kirkwood, L.
Leicester, Bp.
Nathan, L.
Phillips of Ellesmere, L.
Tombs, L.

Examination of Witnesses

MR GRAHAM SMITH, Bird & Bird, and MR HARRY SMALL, Baker & McKenzie, called in and examined.

Chairman

76. Good morning, Mr Graham Smith and Mr Harry Small. Welcome, and thank you very much for coming to give evidence to us. I think it is easiest to start by asking you to say who you are and briefly what you are, for the record, and then I think we will get fairly quickly into the questions, and I know you have had some indication of what they might cover but we will probably range more widely than those particular questions. Mr Smith?

(*Mr Smith*) Thank you, my Lord Chairman. My name is Graham Smith, I am a partner in the London firm of solicitors Bird & Bird and have been since 1985. My professional work includes advisory work and civil litigation in the computer and information technology field and I have done a fair amount of work in advising clients on the problems of converting hard copies to digital images, bearing in mind evidential issues that may arise if those images are required to be used in court. I have also in particular spoken at a series of conferences organised by the British Standards Institution in conjunction with their code of practice on the legal admissibility of digital images and was involved, to some extent, in the preparation of that code of practice.¹

77. Thank you very much. Mr Small?

(*Mr Small*) Thank you, my Lord Chairman. I am a partner in the London and international law firm of Baker & McKenzie and have been practising in the information technology field since about 1981. I practise in the field of civil litigation concerning information technology, particularly the adequacy of computer systems and the issues of admissibility and conversion of analogue to digital evidence. I also advise on questions such as electronic commerce, particularly with regard to the verification and creation of reliable evidence of pure electronic transactions.

78. Thank you very much. If we could start with the first question, I will address it to both of you, and we would like you to speak sequentially rather than at the same time! The first question is, should evidence obtained with security video devices be

treated on a similar basis to that obtained with other equipments, such as speedometers or traffic lights?

(*Mr Smith*) I think by way of preliminary I ought to make one caveat on my comments, which is that, like Harry Small, my experience has been really with civil litigation. I do not profess any experience of criminal cases and I rather suspect that this question comes up mostly in relation to criminal cases rather than civil cases. With that caveat, if I can perhaps extend the question slightly to video and digital images generally, it seems to me that the best analogy, particularly when one is dealing with digital images derived from hard copy originals, but to some extent it may apply to video devices as well, is with taperecordings and photocopies, which have exercised the courts considerably in the past. They raise similar problems of authenticity, quality of reproduction and potential for modification and generally I would regard the differences as being of degree rather than of fundamental kind. The experience of the courts in dealing with issues concerning taperecordings and photocopies, I think, will be highly relevant in dealing with issues such as digital images. If this question concerns, for instance, the presumption which is sometimes applied to machines, that they are working—the presumption of regularity, as it is known—it seems to me that there is really no reason why that should not apply to computer devices as well as other, more traditional mechanical devices, so long as it is borne in mind that the implications of that presumption may actually not be that significant. If one considers, for instance, a scanning device which is scanning from hard copy, the thing may be working perfectly well but there could still be quite legitimate questions about the faithfulness of the reproduction and whether there was an opportunity for it to be accidentally or deliberately tampered with later, and the fact that one may apply that presumption of regularity does not in any way prevent that quite legitimate enquiry being undertaken as well.

(*Mr Small*) I concur with what Mr Smith has just said. One caveat at the beginning again: I am not a criminal practitioner either and what I say is in the context of civil rather than criminal litigation, although, for what it is worth, I am not sure the fundamental principles beyond, of course, the higher standards of proof, should be fundamentally different. Perhaps I might slightly generalise the

¹My involvement in the BSI Code of Practice was in commenting on a draft. I was not one of the named authors of the Code.

6 November 1997]

MR GRAHAM SMITH AND MR HARRY SMALL

[Continued]

Chairman *contd.*]

question as well. It seems to me to be important not to treat the concept of digital reproductions, whether they are digital images or digital reproductions, of any analogue fundamentally differently from existing mechanical devices. The presumption of regularity and questions of authenticity are qualitatively the same with regard to the quality of a second, third or fourth generation photocopy, an ordinary mechanical method of reproduction, as they are, in my view, with a digital scanned image or any other means of digital reproduction. So I do not see a fundamental distinction and I think we should analogise from existing technology rather than view digitisation as something qualitatively different from the existing technology.

79. The fact that there is, in addition to the machine side of all this, a software side to this does, to some people's minds anyway, raise the possibility of manipulation or change which may or may not be fraudulent, but you do not see that as having any significance as far as presenting it as evidence is concerned?

(*Mr Small*) My Lord, no, not fundamentally. The analogue analogy with a photocopy, say, is the fact that we all know that it is perfectly possible to doctor a photocopy by a wide variety of reasons, ranging from whitening out undesirable parts of it to more complex activities. Frequently if one wants to disguise the provenance of a photocopied document, for example, one will white out the line at the top which shows, for example, where a fax has been transmitted. There is software that will do that to digital images or will do more fundamental things to digital images, but I repeat that I do not personally see a difference of degree, it is a matter of proof.

Lord Flowers

80. My Lord Chairman, our witnesses have already implied that equipment and software exist by which images can be modified and this stuff is going to be quite widely available soon, if one wants it anyway, so we have to ask what are the implications of this for the courts? For instance, how easy is it to demonstrate that a digital image has or has not been modified, or perhaps I could put it slightly differently: how cheap is it to show that an image has or has not been modified, because that is how the defendant at any rate might see it, I suppose? I am interested in your general response to the question.

(*Mr Smith*) As with any new technology in the early days while the courts are relatively unfamiliar with these issues, it will probably require a lot of expert evidence if a document is questioned. I think a point that is well worth making is that certainly in the civil courts at any rate large quantities of potentially imperfect documentary evidence are admitted in the courts and not questioned every day of the week. The times when you need expert input are when someone questions a document, questions a fax, whether a fax was sent perhaps or questions whether a photocopy has been changed, questions whether a signature has been forged or not, and then the attention focuses on that document. Expert forensic document examiners come in and so on, but the vast majority of documentary evidence which,

frankly, if it had to stand up to scrutiny by an expert, probably would not pass muster, nonetheless is admitted in evidence quite happily between the parties every day of the week. So I think that whilst it is true in the early days there may be quite significant expert evidence that has to be called where a document is questioned, one should not, certainly in the civil courts at any rate, be too concerned about that because it is actually quite rare for any particular document to be questioned. What I think we must be very careful not to have is a situation where the fear of manipulation is such that we have a rule where no document of this type can be put forward in court until it has been verified by an expert. I think the courts would grind to a halt if we had a rule of that sort.

(*Mr Small*) My Lord, I concur. There is no more reason to have a different presumption for digital images than there is for any other form of image. The reason we are, quite rightly, sceptical perhaps about digital images and digital reproductions generally is the apparent ease of modification. However, as far as I can see, the technology has within it, in fact, rather better means in technically necessary situations to encapsulate within it some form of time-stamping or some form of indication that the image has not been changed since a given date. In fact, we may be slightly better off in some circumstances with digital images which can be time-stamped than analog images such as photocopies or ordinary photographs, which cannot, or rather can

but it can easily be detected. However, the basic principle which Mr Smith has enunciated is, in my view, quite correct, that there is no reason to apply different standards or to apply expert filtration before you accept the validity of a digital reproduction as we would with a photocopy.

81. Just to test you out a bit further, you can have a photograph, an ordinary photograph, and you digitise it and you modify it and you take a photograph of the result. There is no question as to dates or anything like that. You just have another photograph?

(*Mr Small*) True.

82. How do you react to my statement that you have then made a change to a photograph which is undetectable if you do not have the original to compare it with?

(*Mr Small*) I accept that you have made a change that is undetectable but I respectfully point out that once you get beyond the first generation of any photocopy you have no audit trail either, so I am not sure that there is a fundamental distinction again.

(*Mr Smith*) It seems to me that often the real question for the court is not, do you trust the technology but, do you trust the people who have used the technology. Whilst the technology is perfectly capable of achieving this, similarly with doctored taperecordings, with second-generation photocopies, if there is doubt about the document, let us call it that, which is before the court, then someone is going to have to come before the court and give some sort of founding testimony about the provenance of the thing, where it has come from. They are open to cross-examination on that and ultimately I think the question for the court is much

6 November 1997]

MR GRAHAM SMITH AND MR HARRY SMALL

[Continued]

Lord Flowers *contd.*]

less about the technology than about the people who have used it and whether they are to be believed, and that is a very traditional question which the courts have been deciding for millennia.

Lord Howie of Troon

83. A little earlier on, Mr Small, you reminded us of the difference in the burden of proof in civil and criminal cases. How does that affect evidence of this kind?

(*Mr Small*) I think, my Lord, it does not fundamentally affect it, which is why I mentioned it in passing, if you like. The issue, as Mr Smith has said, is really not so much, do we trust the technology as, do we trust the people through whose hands the technology and the documents have passed. Clearly in the case of, for example, a digital—I will call it record—it could be a document or a photograph or anything, a digital record as to which there is some doubt as to its provenance, as to the audit trail, it is obviously going to be much more likely that sufficient doubt for the purposes of a criminal case will be cast upon it than in a civil case, but that, I submit, is a question of burden of proof about people's evidence just as much as evidence of things.

Lord Kirkwood

84. I may be jumping down the list of questions too soon but it seems to me you did make the point that this type of evidence is not generally challenged in the courts. I am just wondering whether that is because of ignorance, perhaps mainly in the lower courts, of how easy it is to fabricate evidence of this sort. Is it ignorance rather than the fact that they do not think there is anything wrong going on? How much ignorance is there in the courts about how easy it is to fabricate evidence?

(*Mr Smith*) I think we are all on a learning curve, even those of us who profess some expertise in the area. So certainly there is room for education of the legal profession and everyone concerned as to what it is they are actually looking at when these things are produced. Although the difficulties are still there: what may be presented to you as a hard copy may actually have its origins in some digitally modified process of which no-one may be aware. In practice, where a flag is often raised is when a witness says, "This is not what happened, that must have been modified or forged" or whatever. You are then put on notice to investigate just what the provenance of the document in question is. Certainly I think it must be right that the legal profession should be educating themselves to be aware of what can be done but, of course, the software to do this, it is not a question of its being available soon, it is available now. You can go into any computer store now and buy software, you can buy digital cameras where the images are loaded on to your PC and the software with which you view those images on your PC is perfectly capable of modifying them. So it is in the consumer realm already.

85. It sounds to me as though the criminals themselves may be more aware of this than the officers of the court?

(*Mr Small*) I would not necessarily like to give the impression that there is complete ignorance of digital technology among the higher judiciary!

Lord Ackner

86. We would certainly accept it.

(*Mr Small*) There are a lot of very IT-literate judges at all levels. Remember that we litigate these issues as between the parties, people litigate whether the software that will modify digital images works or not, because a contract said it had to work or allegedly said it had to work. Particularly in, for example, the Official Referees Division of the High Court there is a lot of expertise, so personally I am not pessimistic, at least in the medium term, about educating all the branches of the legal profession and I think there is a lot of expertise.

Lord Phillips of Ellesmere

87. Could I focus the question in a rather naive way. Suppose that Mr Bill Sykes was under suspicion of doing something nefarious in London and a group of dubious characters said, "No, that is not at all possible because at the time he was at 'The Prospect of Whitby' with us and here is a photograph that shows the group entering the hostelry"? What credibility would then be given to that perfectly genuine looking photograph which had, in fact, been fabricated? Conversely, what would happen if the police said, "No, that cannot be actually true because we have a photograph of Mr William Sykes outside the bank in question at roughly the same time and this is also our evidence." How would the court set about distinguishing or would it simply discount both photographs?

(*Mr Smith*) I think it depends very much on the credibility of the person putting forward the photographs in question and the evidence they have given about how the photograph was taken. We are sitting here assuming these things are undetectably modified. I am not an expert in examining digital images but I rather suspect that as this goes forward so the sophistication of expert evidence in actually spotting indicia in the image as to whether it may have been modified or not will increase. I am probably trespassing outside my own competence here² but I believe, for instance, if you are going to shift someone in the foreground on to a different background, it is actually quite a difficult job to ensure that all the shadows are in exactly the right place. I am trespassing outside my own competence clearly, but it may be that sort of evidence as well, expert evidence as to the picture, will have a part to play.

(*Mr Small*) If I might add one small point, it is a good example of what Mr Smith said earlier, that even if there is a presumption of accuracy of the two

²My comment that I was trespassing outside my own competence was in response to observing Lord Brain indicating disagreement with what I was saying! The Committee may be interested to see the dangers of undetectable modification, also point out the difficulties of modifying some types of images undetectably. The *Scientific American* article goes into some detail on this.

6 November 1997]

MR GRAHAM SMITH AND MR HARRY SMALL

[Continued]

Lord Phillips of Ellesmere *contd.*]

records, we have here somebody through credible means trying to rebut that presumption. When you get to that stage it is a case of, one, looking at the audit trail (if I can put it in that way) of the two records and it is also a case of asking Mr Bill Sykes whether he was or was not outside the bank in question and seeing if the jury believes him, bearing in mind that the evidence that he either was or was not is accepted as not conclusive.

Lord Ackner

88. You could have a position where the court said, "I do not really base my decision upon these photographs because it is quite clear, in view of the conflict of evidence, that either of them could have been faked. Therefore, I have to go to other surrounding matters, contemporary documents of the time, and the inherent probability or improbability of one as to one story being right or wrong." You can have a position where the documents do cancel themselves out.

(*Mr Small*) My Lord, in the case that has been postulated I feel that is exactly what would happen.

Lord Phillips of Ellesmere

89. But the two situations that are conflicting could actually be separate situations and it is something which would need to be applied both to evidence in support of the suspect and evidence provided by the police.

(*Mr Smith*) That is very difficult. A slightly more general point on this is that, as I see it, how the courts have treated documentary evidence over the years, they have had a slightly (if I can put it in a colloquial way) love-hate relationship with documentary evidence, in that documentary evidence is always potentially suspect. On the other hand, reliable documentary evidence is often a very good indicia as to who is telling the truth. We may have a situation where, because of the ease of modification of digital documents, there is just going to be, and has to be accepted to be, a general decline in the reliance that can be placed on contemporaneous, or allegedly contemporaneous, documentary evidence. It may be that that is something that is inescapable and may just become part and parcel of how the courts treat documentary evidence generally.

Lord Nathan

90. My Lord Chairman, may I come back to the question which you asked, which relates, of course, to security video devices which are going to be treated on a similar basis to other equipment, such as speedometers and traffic lights, and my question does not relate solely at all to the criminal field but it also relates to the civil one. We have received evidence that certain codes of practice have been evolved on the principle that public support for the CCTV systems must be secured. The first principle which is before me on this paper from the Local Government Information Unit, who provided this evidence to us, is that: "The information contained in personal data should be obtained from personal data, should be

processed fairly and lawfully." That is a fairly straightforward statement, but it goes on to say: "That means it is important that individuals are aware their image is being caught, the identity of the owner of public systems is made known, and the purposes for which the information obtained by systems will be used is made known." And then it is necessary to require that observations and recordings be relevant and not excessive for the purpose. The question which is in my mind is whether you have any views or experience of the extent to which evidence caught on CCTV cameras could be excluded from being used in evidence if it failed to conform to that code of practice. For instance, if the object of the exercise, what the public were told, was that the CCTV camera was in a public highway with a view to preventing access to a particular area or perhaps general criminal activity such as theft of vehicles or something of that kind, but in fact the camera, either accidentally or otherwise, took a photograph, for instance, in a private place, i.e. through a window, and suppose, for instance, that that photograph was relevant to a civil case, would you accept that that should be evidence in the case or would it be excluded by reason of the code of practice, or is this still an uncertain area?

(*Mr Small*) On the code of practice, first of all I do not actually think it is an area which has attracted all that much judicial attention, but it seems to me on first principles that an image of the sort you mentioned, which could be analogue or digital—I do not think it makes any difference—of a private matter caught through a camera that was designed for other purposes, *prima facie* is a discoverable document in exactly the same way as any other document is and I cannot see any grounds for excluding the normal rules as to the admissibility of documents, civil and criminal, the necessity to disclose documents in civil or criminal procedure, on that ground alone. That seems to me as far as we can take it without perhaps elevating the code of practice to law.

91. I think, if I may say so, you have hit upon a point. One of the things we have to consider is whether there should be any form of legislative control over CCTV and particularly the digital images. Would it be a good idea to have that or not a good idea? The point made to us about this code of practice is that it is essentially to secure and maintain public support and that this will be forfeited if the system is used otherwise than for the sorts of purposes which are indicated here. That is the evidence we have received. I wondered whether you had a view on this. It does relate to the question of civil as well as criminal proceedings.

(*Mr Smith*) Let me put my head above the parapet on this one. I have to say, first, I have absolutely no experience of this situation whatsoever and I have not had the opportunity to see the submissions which are referred to. What perhaps I would be happy to do is, if I could see a copy of it, to submit some views on it later³. I cannot profess to have prepared a view or

³I have received your letter of 10 November 1997 with a copy of the Local Government Information Unit Code of Practice. I will consider this and let you know if I can provide some views on it.

6 November 1997]

MR GRAHAM SMITH AND MR HARRY SMALL

[Continued]

Lord Nathan *contd.*]

a position on something which does raise some substantial wider issues.

Chairman] Thank you very much for that, Mr Smith. We will perhaps take you up on that offer.

Bishop of Leicester

92. We may have moved on a little but I was still reflecting upon the previous example of where one was comparing one photograph with another and, therefore, the spotlight would have been on both photographs. There are perhaps three questions I wanted to ask. One is very often comparing the photograph, let us suggest, with a report, a verbal report. The question then is, because we now know that photographs are so easily manipulated digitally, are the courts aware that they would not now give the weight of authority to this photograph before them that they might have given ten years ago? My second question is, if you were advising the court, what weight of authority would you suggest they give, let us say, to a photograph over against your photocopied document, because maybe it is easier to manipulate digitally a photograph and more difficult to detect if it has been manipulated? Then my third question, the problem is worse than this because surely now almost any document or any photograph can be transferred into digital form and, therefore, can be open to manipulation, so that what looks like a photocopied document might, in fact, have gone through a digital manipulation? I think it is that that I find difficult. What authority can the court give to any image?

(*Mr Small*) The first question was, are the courts aware. In general, my Lord, I think the courts now are aware. The issue has received reasonably wide publicity, the matter has been litigated often in the High Court. My own belief, based on a non-statistically significant sample of the courts before which I have practised, is that there is awareness of the concept of manipulation of digital records.

93. Does this mean that almost any image, therefore, is discounted?

(*Mr Small*) No, it means that the technology is treated with healthy scepticism. I think most people seem to be aware that, although an image does not necessarily have to be true, there is no reason to suppose, on the converse, that every image is faked. It is a matter of degree. It is very difficult to generalise in these circumstances but it is a matter of degree. It is a matter of weighing the digital evidence as one aspect of all the other forms of evidence that there are about what did or did not happen at that standpoint in time and a case, to go back to William Sykes, of seeing what other evidence there is of William Sykes' activities, like what he says he did, what his friends say he did.

Lord Ackner

94. When you talk about the courts in which you practise, are you referring to other than the Official Referee and the Commercial Court?

(*Mr Small*) My own experience is that in general in Chancery Division there is a good grasp of these things, my Lord.

Lord Brain

95. My Lord Chairman, I think it might be quite a good idea if I cleared up question 7, which I think I can do quite simply by asking a supplementary to this. I am going to summarise it. We have been talking about photographs or images produced in positive form. If one goes back, using the chemical analogy, to a negative, can you not seek, if you are presented with a photograph, to go back to the negative? I refer particularly in this case to medical photographs given as evidence in injuries cases and things like that. Can you not equally try and seek to go back to a write once read only memory of the digital image taken either with a digital camera or transferred in a scanned form? Could that not again be a source of evidence? I think this is what we want to get basically down to, where does the evidence start?

(*Mr Smith*) If I may deal with this one, if a party wishes to prepare its documentation to the highest standards so that it can be as sure as it possibly can be that the document will stand up to the closest scrutiny in court, then clearly the way to do it—and the BSI code of practice is very much along these lines—is to put in place formal procedures for either imaging your hard copy originals or dumping your original digital images into the system, putting them on to a non-erasable medium such as a WORM disc, a write once read many times disc, putting that into secure storage and keeping proper records of what has happened to it so that when it comes before the court you can say both, “We have frozen the evidence effectively at the time that we dumped it on to this non-rewritable format”, and also “we have kept it securely.” Clearly that is very good practice. What I think we need to beware of, though, is the reverse of that and saying if you have not done that then it is not admissible, because if you do that you are going to run the risk of excluding the vast majority of business documents which in everyday business at the moment are not prepared to those sorts of standards when we are talking about paper documents. But yes, if you want to prepare your documents to the highest standards and you know that they are going to be used, for instance, in criminal proceedings—I know, for instance, that a particular building society has been doing this for about the last ten years and has successfully introduced its digital images from this system into evidence in criminal proceedings—then yes, that is certainly good practice.

96. Again you have used the words “good business practice”. Good business practice usually ensures that information on computers is regularly backed up and if, therefore, provided the timescale is reasonable, somebody said something happened on 5 November last year, for example, it might be possible to see what was recorded on the computer on that date, even though the evidence is produced subsequently and may have been modified?

(*Mr Smith*) Certainly.

(*Mr Small*) Yes, the back-ups produce a snapshot. That is an important point. I do, however, echo what Mr Smith said, that we must not do the converse and exclude it.

6 November 1997]

MR GRAHAM SMITH AND MR HARRY SMALL

[Continued]

Lord Brain *contd.*]

97. I quite agree. Again one can usually find some way to go back to something a bit better if it is challenged?

(Mr Small) Yes.

Bishop of Leicester] You said that there was a building society which had been doing this for the last ten years. It might be quite useful for us to have details of that at some stage. I find that interesting.

Chairman] Yes, thank you very much.

Lord Brain

98. Could I take question 5. Perhaps I ought to declare an interest here because I am a member of the British Copyright Council and much of what is involved in this could relate to copyright and traceability of false copies and things. It is really this question of audit trails, digital signatures, watermarks and the rest of it. Do you feel this should be achieved by legislation, rules of court, standards, codes of practice or something else, and we are back to whether evidence is obtained on the Internet and, of course, the Internet is being used a lot at the moment legally in another part of the world? Could you give us some broad, quick comments on the situation?

(Mr Smith) My view on this is that if you introduce codes of practice and this sort of thing, the real danger you run is that you shift the focus from the real question, which is, is this evidence reliable, to a rather more sterile question of whether a particular code of practice has been complied with, and I think we have seen that happen with section 69 of the Police and Criminal Evidence Act over the years, which the Law Commission has recommended for repeal. In fact, earlier this year there was a House of Lords case, the case of *McKeown*, which was an Intoximeter case, and Lord Hoffmann, quite rightly given the terms of the Act, started an obiter investigation of whether the time clock within the Intoximeter black box was part of the computer or not. This is the risk you run with this sort of approach, which is that you start to generate artificial questions of that sort. With section 69 we run the risk of having to open up the PC and decide whether the graphics card is part of the computer and whether this or that is part of the computer, which is completely irrelevant to the real question, which is, is the output reliable or not, and I would be very concerned about codes of practice or legislation which could run the risk of that sort of approach.⁴

(Mr Small) I agree. As far as the concept of digital signatures and audit trails is concerned, I personally do not think that one can generalise. When two parties, or many parties, agree to do business electronically, my experience is that there is no real

fixed rule as to the level of authentication of electronic messages and electronic data that one will accept from the other. There are some companies that will quite cheerfully, for example, organise a "just in time" manufacturing system for checking on stock levels and ordering more stock whenever the stock levels fall and they do that either over the public Internet or with quite minimal security, they having taken a risk versus cost-benefit analysis and come up with that conclusion. On the other hand, there are people who will effectively for the same transaction require trusted third parties, quite detailed and technical authentication of each message on a private network. That, it seems to me, is something that should be left to the private legislation (if I may put it that way) of the commercial community.

Lord Flowers

99. If I understand you, the weight of all the evidence you have given us this morning is that there is not much point in challenging the authenticity of the document or photograph or whatever it is, you should challenge the veracity of the witness?

(Mr Small) Yes, in a word.

(Mr Smith) But with the caveat that if an expert witness is able to point to indicators in the document or the circumstances surrounding its creation or whatever, that may very well form part of that enquiry.

Lord Brain

100. Could I make a point that has just come to me. Suppose, without one of the parties realising it, somebody has got into the system and hacked it. Has that ever happened? Is there any evidence that that sort of thing has gone on, that one side has falsified the evidence of the other side intentionally perhaps?

(Mr Small) I personally am not aware of any. I am aware of plenty of instances of hacking in the commercial context from what I might call good old-fashioned credit card numbers over the Internet to more sophisticated things, but I personally am not aware of any occasion when there has been wilful hacking or wilful alteration of documents which are going to be used in court proceedings. That does not mean to say it does not happen.

Lord Tombs

101. May I pursue the analogy of security in commercial transactions, which are obviously highly diverse. Does the same consideration apply to criminal proceedings? I realise this is not your field, but would it not be possible to distinguish between the two, one where a wide variety of commercially desirable transactions is involved and the other where the burden of proof is very important in a criminal case and where there are already in place requirements for storage of originals, tapes of interviews and so on? So could you conceive of two codes of practice, one where the digital evidence may be used in criminal cases and the other where it is used in civil cases or, to pursue that a little further,

⁴Whilst I am not generally in favour of codes of practice, I would not wish my comments to be interpreted as opposition to the sort of code of practice which would govern how digital data should be collected and handled by State law enforcement agents such as the Police. I can see that that could have benefits. What I do oppose is the wider application of codes of practice to private individuals and companies going about their everyday life and business either explicitly, or implicitly by requiring such codes of practice to be complied as a condition of admissibility as evidence.

6 November 1997]

MR GRAHAM SMITH AND MR HARRY SMALL

[Continued]

Lord Tombs *contd.*]

would it be absurd to have a common code of practice in both cases?

(*Mr Smith*) My initial reaction is that it may be adequately dealt with by the different burden of proof. I am reminded of a case called *Cochrane* that occurred some years ago, where the evidence that was sought to be adduced was the printout of an ATM, an automatic teller machine of a building society, and evidence was put forward by, I think, local branch officials as to where the information on the till roll came from and I believe the situation was that on questioning they could not actually say. I should explain there was the local computer on the ATM and it was also connected to a mainframe somewhere. They were not actually able to tell the court in which town the mainframe was situated and this evidence was thrown out, or should I say the till roll was not admitted, and this was at the level before anyone ever got to saying, for instance, would section 69 of PACE apply. It was simply that the founding testimony to support the evidence was just inadequate, and if you are introducing evidence into a criminal case, it seems to me that there is a degree of safeguard in that requirement for having the founding testimony just to get the evidence in in the first place, and that is always going to be probably more arduous a task than in civil litigation.

Lord Ackner

102. Have you had experience of cases where the only material has been the digital material and there has been no proper audit trail and, therefore, no way of establishing the reliability of the material?

(*Mr Smith*) For myself, I do not think so, not yet.

103. If that did occur, would you favour the proposition that the material should not be looked at or merely that it should be looked at with considerable reservation?

(*Mr Smith*) I think I would favour that it should be looked at with considerable reservation, which I think is consistent with the existing approach of the courts to photocopies, for instance, in the case of *Wayte* in the Court of Appeal where this very similar proposition was debated and the court there said that the mere fact that it is easy to construct a false document by photocopying techniques does not render the photocopy inadmissible and it goes to weight. If that is the attitude of the courts to photocopies, then there seems to be no reason to take any different attitude to digital documents.

104. What is your attitude where the images have been compressed or expanded?

(*Mr Smith*) I think that again goes to the weight and the question of how faithful the reproduction is and, of course, the significance of whether it has been compressed or expanded may vary dramatically depending on what type of document it is that has been scanned and what one is trying to prove with it. Clearly if it was an X-ray, it would be the fact that there had been a lot of issues about the resolution at which it had been scanned, whether it had been compressed or expanded. One would be very sceptical indeed about drawing any conclusions about slight shadows on the X-ray and so on. With that, if it was an ordinary business document, a letter,

it might not matter very much at all, and one can see all sorts of shades of grey in between. For instance, a technical drawing may be subject to a process of despeckling, which is one where it takes out the dots in the background. You could quite easily find that that has taken out a very significant dot on a technical drawing and that is, for instance, one of the issues where the BSI warns against that sort of practice. So I think it is very much a case-by-case basis: how significant is the process that is being used compared with what type of information it is, what type of document it is that is being scanned, and what one is trying to prove with it. It is like a fax. Faxes are admitted into court and relied upon every day, notwithstanding the fact that if what you were trying to prove was the time at which the fax was sent, I think we would all be extremely concerned about relying on the reliability of the time-stamp on the fax. That does not mean that for other purposes the fax is not perfectly reliable evidence.

(*Mr Small*) If I may add one thing, that is a very good analogy of how you have to go to the people who created the document rather than the document itself. If I receive a fax from a professional colleague, then I will trust the time-stamp. If I receive it from others, I might not, and I know how to fake them.

(*Mr Smith*) That assumes that your professional colleagues are diligent about setting the time correctly on their faxes, and when the time goes forward or back, doing it.

(*Mr Small*) I would trust them!

105. This, I think, is essentially a matter of what goes on in the criminal courts, but in the civil courts is there any difficulty in obtaining reliable experts to be able to show the potential deficiencies of documents relied upon?

(*Mr Smith*) I think there is an increasing number of experts who would be prepared to—

106. Reliable experts?

(*Mr Smith*) I would hope so. It is interesting because, of course, in the paper world one has forensic document examiners who have for many years examined questioned documents. What I think we are now seeing the emergence of is potentially the equivalent in the digital world of effectively forensic digital document examiners who can look at these. I think we are in the early days. I must admit I for one have not had to make use of one yet, so I have not had to go out and find one. My guess is that I would not have much difficulty in finding someone competent to give a view, if I had to.

(*Mr Small*) I am sure that is right. I have not had cause either. In the general expert community I have no reason to suppose that I could not if I needed to.

107. I do not suppose either of you gentlemen handles legal aid cases?

(*Mr Small*) I am afraid not.

(*Mr Smith*) Very occasionally.

108. Would there be any difficulty, do you think, in getting authority from the legal aid authorities to get an expert once an issue had been raised about the authenticity of what was relied upon?

(*Mr Smith*) I do not have sufficient experience of legal aid cases to know. I would hope that one would

6 November 1997]

MR GRAHAM SMITH AND MR HARRY SMALL

[Continued

Lord Ackner *contd.*]

have no difficulty but I cannot tell you from experience whether that would be the case or not.

Lord Howie of Troon

109. Should you find yourself in a situation where you needed one of these experts, whom do you ask?

(*Mr Small*) I think we all have our list. I use experts primarily for help in analysing performance of computer systems, because that is what a lot of my practice is in litigating. I would go there in the first instance.

110. It would be some sort of institution?

(*Mr Small*) There are various voluntary bodies but there is no sort of Law Society equivalent.

Lord Carmichael of Kelvingrove

111. Is this not going to extend the time taken in the courts and, therefore, the expense considerably with all these documents which need a different method of verification from perhaps earlier days?

(*Mr Smith*) If it is restricted, and in practice certainly in civil litigation it will be, to the occasions on which documents are questioned, then I think probably not. I think it will be dealt with in much the same way as paper documents. It is just that one is

going to a slightly different kind of expert to express a view on it. It may be that as everyone becomes more familiar with the technology we may be able to get into a situation where, as it were, more judicial notice can be taken of the likely reliability or lack of reliability of certain types of document. For the moment I think it will be in the province of the experts, but certainly in the over ten or twelve years that I have been a partner in my current firm, I can think of only one or two occasions on which any sort of document has had to be investigated in this way. I do not see any reason why it should be different with digital documents.

Chairman

112. I am afraid, Mr Smith and Mr Small, that the clock has beaten us but you have been extraordinarily forthcoming with your answers and thank you very much for your trouble and for being so helpful. I think in effect you have really answered the last question, which was, is there any fundamental difference between digital images and other kinds of evidence and I have a feeling on your side of the table anyway there is probably not?

(*Mr Smith*) That is correct.

Chairman] Thank you very much indeed.

Memorandum by Mr Peter Sommer

1. My name is Peter Sommer. I am a Research Fellow at the Computer Security Research Centre at the London School of Economics and Political Science where my speciality is "computer forensics"—the problems of locating evidence derived from computers for use in legal proceedings. My main income comes as a consultant in information systems security; most of my work is on behalf of insurers and corporate investigators and I also appear as an expert witness. My first degree was in law. The views expressed here are my own; research centres at the LSE do not have opinions.

2. The remit of the sub-committee as described on the Call for Evidence touches on a number of areas: provenance of digital evidence, technological capability assessment, technological forecasting, civil rights, press ethics. Each of these areas spawns further issues and I will try to confine myself to matters which appear to be at the core of the Select Committee's concerns or which I feel they should not ignore. In general I will follow the guidance questions provided in the Call, but I will not be saying anything about press ethics as I feel I have no particular contribution to make. The Committee Clerk said that it might be helpful if I could provide some broad sketches of the key issues to give members an early opportunity to decide into which specific directions to take their enquiry.

3. *What is the current and forecast future use of digital technology for image collection, storage and transmission?*

— There are a number of diverse uses and in turn these depend on:

- cost of equipment that can digitise—scanners, screen grabbers, cameras;
- cost of equipment needed to process digitised images;
- cost of suitable storage media; and
- the number and variety of business applications.

— looking at the equipment aspect first:

- flat-bed A4-sized scanners suitable for digitising print and paper originals are now available at just over £100. These are suitable for home and small office usage: for larger organisations where higher levels of throughput and greater robustness are required, costs are proportionately greater.
- a screen grabber is what is needed to digitise an analogue video image so that it can be stored and manipulated electronically. It is a card able to accept video input and which slots into a personal computer. A good quality consumer version now costs about £80. This produces

6 November 1997]

[Continued]

reliable still images and short runs of motion video. For about £350 longer runs of video can be captured and stored: these more sophisticated screen grabbers economise on the amount of storage needed for motion video by using protocols which simply store the differences between one frame and its predecessor. These are either the same as, or very similar to, the techniques used in digital television.

- still video cameras, looking similar to film-based cameras but producing digital files which can be transferred to computer and then printed out cost in the region £300–400 for “consumer” models; professional versions cost £2,000 and more.
- simple but powerful digital editing software is usually included in the price of these digitising devices, though there is often the opportunity to obtain more powerful software for additional cost. Other software also included allows for optical character recognition—OCR—printed text is converted into a form in which it can be edited with a word-processor; again more sophisticated OCR software can be obtained for further expenditure.
- all of these digitising devices, with the exception of equipment to edit moving pictures, operate comfortably on the sort of personal computer sold at between £900–£1,200. An approximate technical specification would be: Pentium 133 MHz processor or better, 32MB RAM, 4MB VideoRAM, 2 GB hard-disk.
- in terms of the costs of storing digital files: file sizes depend on the size of the original image, the amount of detail in the original, the fineness of the digitising scan, whether the image is stored as black-and-white, grey-scale, or any of a number of depths of colour, and the precise data format—some are more efficient than others. Thus the top page of the Committee’s Call for Evidence, A4 size, stored at 400 dots per inch (dpi) in black-and-white produces a file of 70kb. The same page stored as a grey-scale (more suited to a black-and-white photograph at 100 dpi (tabloid newspaper quality) produces a file of 170kb. On the other hand an A4-sized so-called true-color image, capable of distinguishing over 16 million shades and colours, at 600 dpi, and thus almost as good as a conventional photograph, could produce a file of almost 200MB in size. At current prices, hard-disk storage is approximately 7 p/MB.¹ A CD-Writer capable of producing standard 600 MB CD-ROMs which can be read on any computer can be obtained for a capital cost of about £300; individual CD-ROM blanks cost £3–£4. For most purposes other than very high quality colour, therefore, it is cheaper to store copies of documents in digital form than as photocopies in a conventional filing cabinet. And of course there are other advantages, considered below.
- I have spent some time on the cost aspect to show that the technology to produce and store digital images is so cheap that in nearly all businesses and many more prosperous homes digital imaging capability can be acquired without there having to be any specific “justification”. Appendix III contains advertisements and product literature for some of the items discussed above. In making its assessments the Select Committee should appreciate the potential extent of availability of the technology.
- Turning now to leading business applications, I draw the Committee’s attention to the following:
 - *document storage and management*. Paper-based originals are scanned into digital images and then stored and indexed onto data media. The main users are organisations which have a routine requirement to hold large quantities of significant documents for long periods. Examples include insurers, banks, pension companies and much of the public sector. The advantages of digital storage are: compactness, ease of subsequent location of individual items, resilience over time, cost and ease of back-up in anticipation of disastrous destruction of the original. A number of suppliers cater for this market by producing devices that can handle very large quantities of data. These include YMIJS Ltd, NBI, MDi, and Filenet. There appear to be no less than four industry bodies: Document Management Forum, Image and Document Management Association, Legal Images Initiative Consortium, United Kingdom Association for Information and Image Management. On a smaller and less formal scale, a £60 software package called PaperPort DeLuxe and which works with many popular scanners, provides similar facilities—economical storage plus an indexing system for the very small business. The legal status of copies of originals has been eased by the more relaxed definitions appearing in s 8 of the Civil Evidence Act 1995 and s 26 of the draft Criminal Evidence Bill furnished by the Law Commission in Law Com 245 of 1997. In 1996 the British Standards Institute produced a *Code of Practice for Legal Admissibility of Information on Electronic Document Management Systems* (DISC PD0008, ISBN 0 580 25705 4) which the Select Committee will find useful at a number of levels. In particular, if the Committee decide to make recommendations about the handling of digital images in general they should consider ensuring compatibility with these existing standards. I will return to some of these issues later.

¹ 1,000 kb = 1MB; 1,000 MB = 1GB. A 2 GB hard-disk cost about £130 in mid-1997, but prices have been falling at approximately 10 per cent every two months.

6 November 1997]

[Continued

- *electronic publishing.* Two technical developments have speeded up the market for selling digitised images. The first is the CD-ROM drive which is now a standard feature of the personal computer. There is an extensive CD-ROM publishing industry though only a few titles currently make significant profits and most make losses; this phenomenon is usually attributed to: publisher uncertainty about the variety of actual markets for CD-ROMs and poor distribution mechanisms. The second is the Internet's World Wide Web. The market is being held back by worries over copyright protection, both in terms of being able to detect copyright infringement and the problems of enforcing rights in an international market. Methods for the detection of copyright infringement are dealt with below.
- *desk top publishing.* Nearly all magazines and illustrated books are produced in-house on PCs using software referred to as DTP—desk-top publishing. Printers who 10 years ago would have laid the pages out and carry out process work on illustrations, now receive electronic files which contain complete details of how the publication is to appear. An important element has been disk-top image processing software, of which Adobe Illustrator/Photoshop and Corel Draw/Photopaint are leading examples. It is the needs of the DTP industry which has driven the development of these products. They can be used both for simple touching up and much more creatively. There are a number of simpler and lower cost variants.
- *security industry.* The security industry is beginning to make modest use of digitising in the production of identity cards, the maintenance of personnel records, the production of asset inventories and in some closed circuit television applications (considered below).

4. What is its use by the courts and the legal profession?

- The courts and legal professions make very little use of this type of digital storage technology except in the very largest of the complex fraud cases, where documents are scanned and committed to CD-ROM. The advantages are compactness, ease of search and speed up of court proceedings. Changes in the law of admissibility of "copies" already referred to make this form of digitisation easier to accept; it is of course still possible for paper originals to be "produced" in court if required. One leading company providing such services is Legal Technologies Ltd.
- A second use is the production of graphic evidence, for example to show the progress of a fraud and/or linkages between suspects. The juridical problems are: that the graphic may be misleading and that there may be an imbalance of access to resources between prosecutor and accused or plaintiff and defendant.
- The practice does not seem to have extended to slightly smaller-scale cases and this is a great pity. Appendix IV is an advertisement for a company that claims to be able to produce images and searchable text on CD-ROM for the same price as photocopying. One initiative the Select Committee should consider is to urge the Lord Chancellor's Department to encourage the police, CPS and courts administration to move over to this technology.

5. What is the state of the art of image manipulation?

- Others may answer this question more directly but surely from an evidential perspective, the substantive fact to grasp is that the integrity and probative value of a digital image can never be trusted simply on the basis of visual inspection. Although there are many limits to the extent to which a photo-realistic image can be manipulated—it is not possible to state that a digital image has *not* been manipulated or to describe the *extent* of manipulation.

6. Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence? What would be the preferred practical measure?

- Without authentication digital images are worthless. Two technical methods for providing authentication can be considered: watermarking and digital signature.
- The main purpose of digital watermark technology is to protect copyright in images, not to provide authentication. Here is an explanation from one supplier: "Digimarc's digital watermark technology differs from traditional watermarks in that it is imperceptible until loaded into a computer, and can then communicate a hidden message to the reader. This message takes the form of copyright notification, ownership, audience (adult or general interest material), and usage (restricted or royalty free). A Digimarc watermark imitates naturally occurring image variations and is placed throughout the image such that it cannot be perceived. To further hide the watermark, the Digimarc watermarking process is perceptually adaptive—meaning it automatically varies the intensity of the watermark in order to remain invisible in both flat and detailed areas of an image. A Digimarc watermark is durable and survives across file formats and most image transformations, such as copying and editing. Although the watermark is embedded digitally within the image, it remains part of the image even when printed and can be read later simply by scanning the image into a computer." Appendix V provides more detail. This type of watermarking is unsuited to authentication as the watermark is designed to survive editing so as to protect copyright owners whose material is subjected to unauthorised manipulation by others.

6 November 1997]

[Continued

- Digital signature, however, can provide authentication. The original file is subjected to a longitudinal check in which it is processed together with a secret key or pass-phrase. The result, typically a string of otherwise nonsense characters, then exists externally to the image. A third party can authenticate the original by an obverse procedure—the string of characters and the image file are processed against the secret key to produce a positive result. In practice a single secret key would not be used; instead asymmetric public key cryptography would be employed, in which one key is used for encoding and another, the public key which is generally published, does the authentication. In March 1997 the DTI published a public consultation paper: *Licensing of Trusted Third Parties for the Provision of Encryption Services* which *inter alia* discusses strategies and policy objectives for a digital signature infrastructure. Annex A of the paper considers the legal recognition of Digital Signatures. The paper had a mixed reception largely because some of the proposals envisaged a compulsory licensing scheme in which there would be legal access to secret keys used to encrypt messages. Many privacy advocates were uncomfortable about the proposed controls on access by law enforcement agencies. It is a pity that debate on this topic may have slowed down the creation of a generally-accepted scheme for digital signature. During April DTI officials stated that the consultation paper represented the views of the previous government and that revised proposals would be brought forward. The Select Committee should consider speaking to the DTI officials.
- However it is important to appreciate that a digital signature only provides confirmation that two images are identical. They do not of themselves provide validation for an Exhibit nor, in the absence of witness statements or other exhibits do they provide any guarantee that links the images to the events before the court or the probative value of any procedures prior to the creation of the original signature. The BSI *Code of Practice for Legal Admissibility of Information on Electronic Document Management Systems* does not cover digital signature in the way described here—in my view a defect—but does describe certain administrative controls which might be adapted to certain other situations, including digitised evidence.

7. *Under what circumstances and with what controls should modified or enhanced images be used as evidence?*

- The problem is that image enhancement may be presented as being an outcome-neutral “scientific” process when in fact a technician may have to employ a considerable amount of interpretation. In general terms image enhancement does not so much reveal information that is hidden in an image as to make guesses: a case in point is “image sharpening” where the program examines an image for relatively significant transitions of tone and then creates a line of black pixels (picture elements) between them to make the transition appear more definite. This and other controls may have to be used selectively in order to get a “realistic” enhancement.
- Image enhancement is at its most uncertain when it is being asked to produce results from very poor originals. In a typical situation: an image is originally available from a low quality black-and-white security camera sited in a room with poor lighting and an incident of interest has been recorded onto a video recorder on which the regular recording standard has been reduced in order to permit a slower-than-usual recording speed so that tapes do not need frequent changing. The item of interest is the face of a human being; the camera shot is from considerably above eye height and the critical face occupies perhaps two per cent of the total screen shot. The “best” still from a sequence is then digitised by a screen grabber but in the process the analogue video scanning line interferes slightly with the horizontal dot rate of the digitised image, thus creating an interference. Assuming that the digitising process turns the analogue video into a full-screen VGA image of 640×480 pixels, the face itself occupies about 6,000 pixels (say a square of only 75×75 pixels) and it is from this that the technician must prepare an exhibit. There is particular danger if a technician is asked to match the image against a known suspect.
- The Select Committee will probably wish to seek opinion from the Forensic Science Service.
- My recommendation is that such evidence should only be considered when:
 - the unmodified original image is provided together with the alleged enhancement and an explanation of the hardware and software used to carry out the enhancement plus the availability of the technician for cross-examination.
 - experts appointed by the person against whom the enhanced image are offered access to test the equipment used for the enhancement for the purpose of aiding any rebuttal.

8. *Do technologies which compress data or use error correction technology when transmitting it raise special problems?*

- In general terms, no.
- Error detection and correction are used throughout computer technology sometimes invisibly as when data is recorded and retrieved from hard-disk and sometimes more explicitly when error correction protocols are used for communications between computers. Their presence increases the integrity of the process.

6 November 1997]

[Continued

- Data compression is used in most forms of image file storage. If a black and white A4 image is scanned at 300 dpi, some 8,750,000 dots, either black-or-white are registered. However the image can be described in many fewer bits of information by counting contiguous blocks of black and white matter or indentifying mathematical patterns. The different image file formats used in the computer industry use a variety of means of image description. Whilst it is true that the most extreme forms of compression run some small risk that image retrieval is imperfect I imagine that any party seeking to rely on an image for evidential purposes is unlikely to run any risk by using a contentious compression method.

9. *Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties? Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?*

- The main civil liberties issues in relation to cctv apply equally to analogue images. Nearly all current surveillance video is analogue in nature and stored as analogue signals. The main issues are: camera placement so as to avoid intrusion into private rooms and offices, controls over who has access to the live video feed, controls over the accuracy of the marking of any on-screen identification information such as location and time/date, controls over who has subsequent access to any tapes. Some of these issues are addressed in the Local Government Information Unit publication: *A Watching Brief—a code of practice for CCTV* (HMSO, 1996, ISBN 18979 5719 X). This is a voluntary approach which might form the basis of statutory controls: authentication and chain of custody issues might be added. Alternatively it might be appropriate to issue a Code of Practice under the Police and Criminal Evidence Act.
- The above considerations apply to surveillance cameras located in public places. As far as video surveillance on private property is concerned, I would like to think that this would be included as “interference with property” for the purpose of section 92, Police Act 1997 which provides a framework for the use of bugs. The Select Committee may like to ask the Home Office and the National Criminal Intelligence Service for comments. I do not know whether the Commissioner referred to in section 91 of the Act has yet been appointed.
- Turning to image tracking software: the best-known application involves the recognition of vehicle number plates from video cameras placed over main roads and the correlation of data with the DVLC and special purpose mapping and tracking software. I am not sure of the current state of face-recognition software; again perhaps the Forensic Science Service has better knowledge. Any new form of surveillance is a potential threat to civil liberties as each usage has a cumulative effect. On the other hand, if one were to rate the existing technologies in terms of levels of intrusion, this particular form of image tracking software would probably come rather low: below telephone tapping, bugging, opening of mail, inspection of bank, tax and health records, eavesdropping on e-mail. The tracking of vehicles through number plate data is done from public places and is scarcely different from following an individual on foot. Given that the method is only effective against a large capital investment in camera sites and computer technology it seems likely that actual use will be limited to the police and security services. Precautions against abuse could include: a requirement that all usage is recorded together with specific reasons for authorisation, extent of actual usage and outcome. This record could then be made available to an independent Commissioner who would make an annual report. This control mechanism would be similar to those existing in other areas such as the Interception of Communications and the Security Service.

10. *Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?*

- This seems to be an obvious good idea: my experience as an expert witness in cases involving other forms of computer-derived evidence has been that whilst there are a small number of enthusiastic and knowledgeable police officers and CPS staff, levels of knowledge about the seizing and handling of computer data and the reasonable requirements of the defence in relation to disclosure are patchy. Perhaps the same might be said of counsel and Crown Court judges: there is a growing

6 November 1997]

[Continued

number of well-informed individuals but it is my view that all concerned in the criminal justice system should have regular briefings on relevant new developments in computer-related evidence and investigations.

I would be happy to enlarge on any of these issues.

Peter Sommer

4 August 1997

Examination of Witness

MR PETER SOMMER, London School of Economics, called in and examined.

Chairman

113. Good morning, Mr Sommer. Thank you very much for coming to give oral evidence. You have already supplied the Committee with very helpful and thoroughly well presented written evidence, for which we thank you very much indeed. For the record, perhaps you could say who you are and we will ask if you have any opening comment you would like to make before we go into our series of questions?

(*Mr Sommer*) Thank you, my Lord. My name is Peter Sommer and I am a Research Fellow at the Computer Security Research Centre at the London School of Economics. I am a part-time academic. My income comes from doing risk analysis for the international insurance market, where they have complex risks where there are strong computer elements, and because my first degree was in law, I do a fair amount of expert evidence, mostly in the criminal courts. I noticed that many of the questions which your Lordships were asking of the previous witnesses were related to those, so for those people who wanted to seek out someone who does the expert work, or tries to, then I hope to be able to answer your questions and I very much hope that some of the questions that your Lordships put before the previous witnesses you will be good enough to repeat to me because I found myself in some frustration not being able to stand up and answer.

114. Thank you very much for that, Mr Sommer. Can we start with the first question, whether evidence which has been obtained by security video devices should be treated on a similar basis to that of other equipments, such as traffic lights and speedometers?

A. I think I have two observations to make. First of all, English law makes a distinction between rules of admissibility, in other words, decisions that the judges make about whether evidence should be examined as a matter of fact and the weight of evidence. In fact, your adviser sitting next to you is one of a number of people who have written interesting learned journal articles about that confusion. I think in answering this question and also in determining what recommendations you might make as a Select Committee, you have to draw that distinction. Clearly there is a wide range of things that should be properly left, as a matter of fact, to the jury and one has to ask oneself how far it is appropriate for the law to try and impose a series of rules which will in some respects constrain what they are doing. On the other hand, you can understand that with complex evidence, evidence of a complex nature, it might be necessary to think of ways of protecting a lay jury. To answer the question specifically, the law has in recent years tried to draw a

distinction between computer evidence that is drawn from very simple single-purpose devices, such as a speedometer or an intoximeter or even a traffic light, and from general purpose computers. In the first category it is called real evidence, and that is used in a rather technical sense, and you will have heard other people refer, and in my written evidence I also refer, to section 69 of the Police and Criminal Evidence Act. Real evidence does not come under the rules of certification that will have to be applied under section 69 and all other types of evidence. My own view is that material from a security video device is not simple in the same way that an Intoximeter is, because it is capable of considerable manipulation, whereas with an intoximeter or a simpler counter or simple weighing machine, either the device is working or it is absolutely manifest that it is not. I think I might also say at this time that I think—and I am anticipating some of the other questions I think you may be asking—one of the distinctions between computer evidence and a lot of other types of evidence is that intrinsically computer evidence is not visible. It can be rendered visible in certain circumstances. So there may be a case for saying that there should be special provision for material which in its most fundamental form is not visible to the jury, in other words, cannot be demonstrated, whereas for most other types of evidence there is something visible which can be put before a jury and you say, “Members of the jury, can you see this is not one and the same thing?”

Lord Flowers

115. Can we start from the point of view that the equipment and the software already exist to muck about with images to our heart's content, perhaps with criminal intent. Would you like to say a few words about the implications for the courts of this? You heard us ask before a number of

questions that flowed from this and if you care to answer some of them now that would be fine, we would be very grateful.

A. Let me, first of all, address the issue of the wide availability of this equipment. The current cost of a flat-bed digital scanner of modest domestic specification is just over £100. For your £100 you will also get some reasonably good photo manipulation software; in fact there is scarcely a computer-owning home in the country and certain no business in the country that uses personal computers in one way or another that cannot buy in this sort of equipment for extremely occasional use, almost as a toy, without having to do any serious business justification. That is the first big fact that I think you have to take in

6 November 1997]

MR PETER SOMMER

[Continued]

Lord Flowers *contd.*]

mind. The second thing is that certainly as far as the criminal courts are concerned, the real issue about any form of evidence is doubt. It is the fact that something could have been manipulated. The fact that a defendant or an expert acting on behalf of the defendant can stand up in court and say, "We cannot be sure," may be enough, in the absence of other sorts of control, to close off the credibility of a particular item of evidence. I do not think that is grounds for saying routinely that we should not be accepting this type of evidence, but it does seem to me that, as with other types of evidence routinely brought before the court, what is going to count is the audit trail and that can simply be an audit trail of witness statements of people involved, and if you look at a typical bundle of exhibits of witness statements that are produced in any substantial criminal trial, there are usually very large numbers of almost trivial but nevertheless important statements from officers who carried out a seizure, officers who have listed items that have been carried away, documents from forensic examiners together with hand-over documents saying the evidence has been preserved and so on. There is quite a large paper trail and in some respects it looks rather tiresome. In the majority of cases there is no need to question them but certainly from the point of view of the defence the existence of this audit trail of activity gives a great deal of credibility to something that otherwise one might worry about a great deal. I hope that answers your question. You were, I think, asking me a whole range of questions and I am willing to be prompted about anything more specific.

116. I think the only other question I would like to ask at this point is to do with the expense of challenging the authenticity of a photograph or document or whatever, especially from the poor old defendant's point of view, who may not be particularly well off.

A. There is a legal test for defence disclosure which is defined in a case called *Keane*¹ where you have to show that anything that you want to do is going to be material and there are various fairly elaborate tests. That is one sort of control. The other control is the one to which Lord Ackner referred in one of his earlier questions, which is the reaction of the Legal Aid Board. Normally the approach that I would take to a complex case, when I might be dealing with instructing solicitors who know they need advice in general but do not know quite what that advice is, is to be asked to be allowed to carry out a preliminary overview of what the issues might be and then produce a specification of what seemed to be material. That would then be couched partly in technical terms and partly in legal terms, and based on that then counsel could write an Advice saying that they agreed with my view or select a version of my recommendations and that would then go forward, and that does represent, it seems to me, a sensible control on the costs. Plainly there is no point in trying to question absolutely everything. On the other hand, in criminal courts, in contrast to the civil courts, we are in a very adversarial situation. In most cases obviously you are not depending solely on the digital evidence. Counsel will decide whether they are

going to concentrate on the material that I as an expert can produce or whether there are other extrinsic factors which are going to be more important. That is how it happens in practice. I do not know whether that gives you any comfort.

Lord Brain

117. We are now turning to the point you have just been making, to a certain extent, of audit trails and digital signatures, the base as to where the image comes from, how it can be traced, and should there be legislation, rules of courts, standards, codes of practice or something else? Then the sub-question is the Internet, which I think probably on the criminal side is of less importance. Also we recently went to visit the City Police "ring of steel" where we saw all sorts of images on television screens which they said were, or could be, recorded. To what extent do you feel that this needs an audit trail and things like that?

A. Let us deal with the issue of codes of practice, in the first instance. In contrast to the evidence that you heard from the solicitors who preceded me, who practise mostly in the civil courts, I am in favour of codes of practice. I think probably the most appropriate way of doing it would be under sections 65 and 66 of the Police and Criminal Evidence Act, where the relevant Secretary of State, in this case the Home Secretary, is allowed from time to time to issue codes of practice; examples include the seizure of goods, handling of tape-recorded interviews. It seems to me a good principle, a good way of handling a difficult situation where you need to reconcile the privacy, the sanctity of the individual and the needs of law enforcement; the code of practice, it seems to me, has a great advantage over primary legislation in that it may be discussed in rather more detail. It is a question of confirming by the spirit rather than in the letter, and over a whole range of computer-derived evidence, not only digital images but the seizing of computers and the printing-out of documents allegedly from seized hard disks and so on, a whole range of things, it seems to me nobody knows quite what to do. There are various bits of kit that are available to law enforcement that one has become aware of. There are conferences held by law enforcement officers and sometimes people like myself, who act primarily for the defence, get invited to them. Everyone, I am convinced, is acting for the best. Nevertheless the controls really are not there. I would certainly like one of the recommendations that the Select Committee makes to be that a code of practice in relation to the handling of computer-derived evidence is produced. A primary feature of that code of practice, it seems to me, would be the creating of various audit trails. I think you raised an interesting question of the point at which the audit trail starts, and a code of practice would not answer all the questions but it could identify duties of various people at various stages and perhaps suggests various forms of documentation or depths of documentation they ought to produce, and I think that is the way forward. You also mentioned the role of digital signature. First of all, I think I need to identify two different uses of these phrases "digital signature" and "digital watermarking" because they

¹Times Law Report 28th April 1995

6 November 1997]

MR PETER SOMMER

[Continued]

Lord Brain *contd.*]

become a little bit confused. What I in my evidence capriciously refer to as “digital watermarking” is a technology which embeds information in an original image such as to try and protect the intellectual property in it, and from what I understand of your interests, my Lord, that is a particular interest of yours. What you are trying to achieve with that type of technology is, even if the image is manipulated, nevertheless there is some record left to show who the original copyright holder was. In a legal situation, in a criminal evidential situation, that is not what you want. What you actually want is something that is going to say that something has not been altered and for that purpose I personally would use the term “digital signature”. That would then be something that is not embedded intrinsically in the document but would be an extrinsic string of characters which represented the digital signature. In that connection I would draw your Lordships’ attention to the work of the Department of Trade and Industry who produced a paper on Trusted Third

Parties for the handling of encryption earlier this year. In my written evidence I give the date—March 1997. That document has been received with some controversy, largely because in addition to the very worthwhile suggestions about digital signature, which are helpful, I think, in the context with which your Lordships are concerned but are also of great benefit in electronic commerce. There were separate issues about law enforcement and intelligence agency access to encrypted data and the same technology would be used for digital signature as for encrypting; in other words, completely hiding communications. I and a large number of people would like to see the two proposals for digital signature and the issues of what the law enforcement and the intelligence agencies need severed. I think they can be severed. I am in no way hostile to the requirements that law enforcement might have in relation to encrypted information but it does seem to me that the controversy that has been created is preventing us from having digital signature, which would help us to provide in a very practical way the audit trailing that I think is going to be essential for digital images and other forms of electronically originated materials.

Chairman

118. Could I take you back—and it follows, I think, from that—to your point about the value of codes of practice, which generally apply to systems which have had some form of approval. If material which is important to a criminal case is obtained from without those approved systems and, therefore, may be without the code of practice, does that suggest to you that that sort of material might not be very valuable because it does not fall within a code of practice?

A. That would be a matter of weight for the jury. It would depend on presentation. Inevitably in a whole range of cases where material is seized from a computer, some of the computers that are most interesting are probably not approved and do not conform to some BSI standard. I think it would be enormously unfortunate if a computer had been seized from a criminal or a drug baron—I have

handled material from that for Customs and Excise—or from a hacker and one was saying that *de facto* because it did not follow a code of practice one should not be looking at it. Plainly it would be a question then for argument before the jury and what experts on both sides would say. But, for example, I have a case right at the moment which involves paedophilia. The police have collected the evidence. They did not preserve the evidence quite as well as they might have done and one could criticise them on those grounds because there is a sort of informal code of practice even if it has not been enshrined. Looking at it in all honesty I have great difficulty in saying that although they were a little bit clumsy this is grounds for having that evidence wholly withdrawn from the jury. It would be a matter of degree, and if one might have an analogy with a routine scene of crime, you have a body with a knife in its back and adjacent to the body is the imprint of a policeman’s boot because he was a bit careless, but it is just one policeman’s boot and one can clearly isolate it. The policeman is available and says, “I just had a look and I’m sorry I didn’t wipe my feet beforehand.” On that basis you would accept it. On the other hand, if the policeman had gone over and waggled the knife to see how far it had gone in and he had failed to

record it adequately in his notebook, then presumably that would be rather less credible, so I think one would presumably take a similar approach with this sort of evidence. In other words, to echo what was said by some of my predecessors in this chair, it is still a question of believing the individuals who have collected the evidence, but they can use the technology and their notebooks and a formal process greatly to bolster their credibility.

Lord Ackner

119. What attitude do you take when the sole material is the digital material and it is open to suspicion? Do you say it should be ruled out or it is a question of a careful direction to the jury?

A. I think it is very much a matter of bringing it before the jury. My inclination is very much to put as much before the jury as possible and I would regard it as the duty of the experts not only to be expert, but they ought to explain things in simple terms and do so honestly and clearly. I would not want to remove things artificially from the jury in the way that has been done traditionally under section 69.

120. If the material was intrinsically so difficult to understand and follow, that might be a basis for saying, “This should not be admitted”.

A. Well, I think perhaps we might take the analogy of the debate that has been going on in the cases of complex fraud trials and you will recall that Lord Roskill in his report was in favour of dispensing with the conventional jury and in favour of having expert assessors; there was a debate at the time and people decided in favour of the jury. In fact that debate has resurfaced again and we may be facing a not dissimilar situation. All I can say, based on my own experience and perhaps my own inner urges, I would prefer this to go before the jury and I think once you start having expert assessors, there is then the question of how you decide that they are experts.

6 November 1997]

MR PETER SOMMER

[Continued]

Lord Ackner *contd.*]

121. With your knowledge and experience of criminal trials, do you find that there is really a need for education of the judiciary and of counsel on this really rather complex subject?

A. My experience is that knowledge is very patchy. Plainly if you have an expertise, a rather bizarre arcane expertise in the way in which I do, then you feel that everybody ought to know a great deal more about it, but if I can move away from that rather obvious position, I have found that there are a number of judges who are extremely knowledgeable and capable, I have found that there are counsel who are available and in terms of solicitors, I think the real thing for the solicitors to do is to identify that they have a problem and to learn how to instruct the expert and it is not just going to the expert, but knowing what they want the expert to do, and to manage the expert properly. There is plainly a danger that the expert simply runs away with all sorts of fanciful theories, billing the Legal Aid Board at a large hourly rate and to no particular purpose and I would certainly like to get some modest training together for people to develop an understanding to a minimal level. In that connection, one of Professor Chris Reed's colleagues and I have been trying to set up seminars which we hope to do which are designed precisely to help in this form of education and to discuss some of the issues that we have been raising that I have been mentioning today.

Lord Phillips of Ellesmere

122. Could I follow that up with my question about expert judgments on whether or not digital photographs have been tampered with? People become extremely expert, as I understand it, in the use of computer programs to modify images. Do you think the real experts in this field can produce a product which another expert would find very difficult to identify whether internal evidence has been tampered with?

A. The problem really is the degree. In other words, it is relatively easier to carry out a small, perhaps significant change than a large-scale change. In other words, if you want to have a real-life, fully-rendered picture of a dinosaur shaking hands with your Chairman in this room, then you would have to work jolly hard to do so. On the other hand, if we had a photograph of your Chairman and wished subtly to change his tie, perhaps the colour of the tie he is wearing and then draw some adverse conclusions, I have no idea quite what that might be, then that would be easy. So there is no straightforward test certainly in the terms of the more complex manipulations. If I can go back to the awful problem of paedophilia, one of the things that happens quite frequently is that images are manufactured, that people take a relatively innocent picture of an under-age child and then superimpose on to that some of the characteristics of a much older person and you end up with a manufactured image. I have unfortunately had to see a number of these things and on the whole, quite apart from the peculiarity of the anatomical results, if you see what I mean, you can normally tell. That is not answering your question directly, but I am saying that it is possible to

do all sorts of things and to a certain extent expertise can help. It is like any other form of expertise; there are limits and the limits change all the time.

123. But if we go back to my earlier example of incorporating a suspect's image in a group photograph, let us say, maybe in the back row, just a head between two other heads or something, can you conceive of a real expert doing that in a way which could actually be detected?

A. Yes, that was the technique famously used by the old USSR, though I think on the whole they tended to remove people rather than add them in! Yes, I think people can produce stuff which would persuade a jury and that would be in terms of looking at the edges of the image where it might have been altered and looking at differences of shadowing and lighting. In a way, I think the big problem with digital images is not the one that you are highlighting, but it is one where you are starting off with poor-quality images, such as you might get from a security video, and then someone is saying that they are enhancing it and the enhancement is given a whole array of scientific names where in fact the software is giving you so much flexibility that, whether they realise it or not, the technician is in fact painting an image to suit, and the scenario I would urge your Lordships to consider is not so much the malicious one as the well-intentioned mistake. It seems to me, in terms of the big forensic mistakes that have led to the well-known miscarriages of justice, that it has been the well-intentioned mistake that has been proved to be the problem rather than the directly malicious behaviour.

124. Could I, my Lord Chairman, pursue this one stage further back? Suppose we have such a very professionally concocted photograph to be adduced in evidence and someone says, "Well, here is a print, but where is the original?" Would it really be difficult to manufacture a seemingly original, read-only memory disk from a digital camera which represented that photograph?

A. We would come back there, I think, my Lord, to the audit trail. I always draw a distinction in computer-derived evidence between what one is being offered to look at, the content, and the process by which it has been produced in court, and it might be quite a long story. In the case of a digital image, you will start off with a camera and you would want evidence from someone who set the camera up and perhaps collected the tape or the image from it and you would want an audit trail of what had been done to it since. Now, the courts have considered a related issue which is non-scientific evidence in relation to DNA material. In other words, this problem of the courts having to consider a new scientific technique is actually not a new one. Indeed there was a case relatively recently in the Court of Appeal, or a pair of cases—and if I might have your indulgence, I will undertake to provide you with the details for the record² because I cannot remember them just off the top of my head—but the outcome of that again was the suggestion that there should be an audit trail and also that the defence should have adequate access to

²R. v. Dohenny, R. v. Adams (Times April 1996, Court of Appeal)

6 November 1997]

MR PETER SOMMER

[Continued]

Lord Phillips of Ellesmere *contd.*]

all the individual stages and any specialist software and so on. In other words, the test is that a defence expert, having shown adequate justification for it, should be able to look at all the stages and reproduce what was being done to his satisfaction and if he cannot do it to his satisfaction, then he must go before the jury and explain why it is not and why the jury should discount it.

Lord Howie of Troon

125. Mr Sommer, you are clearly an expert in these matters, but in your opening statement you remarked that your first degree was in law.

A. Yes.

126. I wonder what you did after that to acquire this expertise.

A. I have had a rather bizarre career. I read law at Oxford and I spent three months deciding that I did not want to become a solicitor. I then went into book publishing and published paperbacks. I always had an interest in science and technology and about the time that people started talking about microprocessor, I decided to take the amateur radio exam as a way of, if you like, finding out about the technology where the arts degree system as it then existed does not help you. Then I fell among people who were interested in the early days of home computing and when British Telecom's Prestel started, I then moved from book publishing into electronic publishing and suddenly had to learn a great deal about computing. I am self-taught in computing. In 1984 I wrote a book on computer hacking at the suggestion of a book publisher and because I was fortunate in the timing, it got into the bestseller list and then people started asking me to act as a consultant in the area and I then started to move, if you like, into the expert witness area and my legal background plus my knowledge of computer technology stood me in good stead. I am sorry for the long answer, but that is the only way I could answer your question, I am afraid. In other words, it was not a very straightforward career, but if you see it in the detail, it has got some sort of bizarre sense to it.

127. As a fellow publisher, if I may ask, would it be fair to say that you are actually self-taught?

A. In computing terms, I am self-taught, yes. In other words, I did not go to university and do computer studies, but in fact the department of the LSE to which I am attached now is information systems rather than computer studies. We turn out analysts and consultants rather than programmers. I can do a small amount of rather poor-quality programming.

Lord Brain

128. Following up Lord Phillips' question, is not part of the audit trail if you are looking at what I call chemical, in other words, traditional photographic film, that you look at a series of negatives and see that the one that they are presenting as evidence is consistent with the series of other pictures and exactly the same can be done with a digital camera and things like that, can it not? In other words, if you

happen to have, as Lord Phillips said, an image which you have reconstructed, you would really want to see what was photographed before and after on the same electronic source.

A. With respect, I am not sure that your analogy entirely works because a digital copy is exactly the same as a digital original for most purposes. Your problem is to try and prove that one is the copy of the other and that is where the digital signature providing underpinning technology and the audit trail of witness statements is going to support you. You prompt me to ask again about the Internet because you raised a question on that and I would like to take that.

129. Certainly.

A. I think in your question you seem to think—was it your suggestion that the Internet was somehow different?

130. I was thinking perhaps it was rather more difficult to get the genuine digital signature and audit trail if you started with an image off the Internet which you had downloaded and things like that.

A. I have recently written a journal article, and again I will provide you with the reference*, and in fact I think I provided in my submission to you a rather perhaps overlong explanation of what the problems are, but we are seeing evidence coming from the Internet. I have a number of cases in which most of the evidence is from the Internet at the moment and there are profound difficulties and we are struggling with them at the moment.

* (1997) *Journal of Financial Crime* 5 JFC2, 138-151

131. We started from the point where a £100 scanner took an image and fed it into a computer system and it goes into active memory. It may then, as you suggest, get manipulated. Where do we start with the electronic storage? How do we trace it back to a point of original electronic storage? We were talking earlier about WORMs and things like that. How do you feel we need to put in some measures to determine the value of computer-processed images and documents?

A. I think the answer really there is something remarkably similar to the proposed British Standard for document image systems which we have heard reference to and I am broadly familiar with the Standard. In fact Graham Smith, whom you heard from earlier, and I even spoke at the same conference a while ago on the subject. It is a question of the audit trail, having a clear procedure and, as I said, backing it up with some sort of time-stamping or digital signature as an underpinning technology. For a whole range of the questions that you are asking me, it is having an auditable procedure underpinned by technology which I think is the solution really. However, you come back to where anything is audited, ideally the audit provides such a degree of corroboration that it is impossible for people to lie or if they do lie, then in cross-examination that becomes visible to the jury.

132. Could I just follow it up slightly really as much to get the information on the record. To what extent are there computer-based systems that will enable you to compare one image or document

6 November 1997]

MR PETER SOMMER

[Continued]

Lord Brain *contd.*]

against another one that is produced in a computer form? It is like using a spellcheck against a document you are typing. Are there other similar systems that can scan two images and say, "The colour has been changed here", the colour of the Chairman's tie, for example?

A. With respect, it would not happen quite in that way. You would actually have two electronic originals, two electronic documents and you then want to compare them and that is extremely easy and there are plenty of utilities to do that.

133. I thought so, but I wanted to have it on the record.

A. Fine. There is no technical problem there at all.

Lord Ackner

134. Do you take the view that there are fundamental differences between the use of digital images as evidence and other kinds of documentary evidence?

A. I think the only fundamental difference is that the digital image starts out as something that is invisible to the human eye and there may, therefore, be a case for warning juries that they have to apply an additional range of tests before they accept them, but in general terms I do not think there should be any distinctions and I would not want to try and elevate it too much. It is still, I think, a matter for the jury. The distinction I would make is the one that I referred to earlier on, that you urge the jury to think not only about the content of what they are looking at, but the process by which the print-out has arrived in front of them and whether they are entirely happy about that process.

135. If you are dealing with an identification case in a criminal trial, what sort of warnings should one give to a jury where you are relying on digital material?

A. Is this perhaps the enhanced closed-circuit television image that you are thinking of, my Lord?

136. Yes.

A. I think what you have to say to the jury is, "Members of the jury, what you are seeing on screen or being offered by way of print-out has been digitally enhanced. The Crown are going to be claiming that this has been a scientific process, that such manipulation which has taken place has been done honestly and scientifically for the sole purpose of revealing material that you cannot quite see with the naked eye. You should not accept it absolutely at face value, but you really need to know about the camera, you need to know how good the original camera was, what sort of digital processing took place, what sort of controls took place and the defence are going to be cross-examining their expert and you should pay particular attention to him".

Lord Flowers

137. Mr Sommer, I do not quite understand the distinction that is being made about images which are visible or invisible to the human eye. A photograph is invisible to the human eye until it has been processed. A microscope picture is invisible to

the human eye until you look down the microscope. What point are you really making?

A. I think the point I am making is that it is a combination of things: first of all, that the raw digital image is in a purely electronic form; and, secondly, the fact that it has changed is rather more difficult to establish than it is for almost everything else. I was saying I did not want to push that problem too far. I think those twin facts—

138. So it is still a matter of degree?

A. It is still a matter of degree and I come back to what I was saying earlier on, that I think there is a delicate balance to be struck between having rules of admissibility, possibly codes of practice which would be, if you like, part of legislation, but which would be delegated legislation, as it were, and leading things to the free admissibility principle and, therefore, before the jury as a matter of fact, and ultimately that is going to be a pragmatic decision.

Chairman

139. You make the point in your written evidence about some of the dangers of compression techniques and methodology and that some of the more extreme types can lead to distortion. Does that, to your mind, make it important that the court should be presented with unenhanced images as well? Do you see a particular issue here?

A. I certainly believe it is important that the defence has access to all the stages that something might have gone through as far as possible and insofar as they do not have access to all the stages, that would give them grounds to draw that to the jury's attention. If we are looking at the specific problem of compression, there are degrees of compression, some of which are regarded as almost perfect and some are to a certain extent glossy. Again if we have got a proper audit trail of what was done, then I believe it would be up to a defence expert to advise his instructing solicitor and counsel whether he thought something should be made of it. In other words, I think the important principle I am urging on you is auditability of procedure rather than trying to say, "This technology is good and that technology is bad and we ought to have separate rules for it". The expert, and the defence expert in particular, should be able to look at what was done and decide whether it is going to be important.

140. From your experience, do you think the courts have generally got a sufficient feel for this area in order to be able to challenge images in a convincing way if that is necessary?

A. Well, the practical problem really is whether the defence solicitor in the first instance realises that there is a potential for challenge and then counsel and then instructing the appropriate expert to do the appropriate work. That really is the fundamental problem. There are a small number of legal problems which we have discussed relating to section 69, but hopefully the particular contortions that section 69 pushes us through are not going to be with us for very much longer, as soon as Parliament can find time to get rid of it.

6 November 1997]

MR PETER SOMMER

[Continued

Chairman *contd.*]

141. Are there any other questions? No. Are there any other points, Mr Sommer, which you would like to make in the few minutes we have available?

A. No. I was very flattered to be asked and there were a number of issues which I hoped to be able to get raised on the public record and fortunately the

questions you have put to me have enabled me to do so.

Chairman] Well, thank you very much indeed and once again thank you very much for the very full written document which you gave which we all found most valuable. Thank you very much indeed.

THURSDAY 20 NOVEMBER 1997

Present:

Ackner, L.	Flowers, L.
Brain, L.	Hogg, B.
Carmichael of Kelvingrove, L.	Kirkwood, L.
Craig of Radley, L.	Phillips of Ellesmere, L.
(Chairman)	

Memorandum by the Local Government Information Unit**PRECIS**

Safeguards are required in the use of data from CCTV in evidence. It will be necessary to set a reasonable standard, and to make meeting this standard a requirement of law. The standard should apply to both analogue and digital recordings: approval can be given to methods of achievement that are appropriate to the system of recording. The safeguards should ensure uniformity across production and storage of the data. It will be necessary to set up an independent body to establish standards, as these are technical matters on which the public cannot make a decision. It will be necessary for the industry to agree that the standards are practical and for a technical committee to agree that they are safe.

The main civil liberty issues raised by CCTV are as follows: the protection of information about individuals and the relevance of standards found in the data protection regime; balancing the public interest in the use of CCTV; enforcement of identified standards in the absence of a relevant legal framework for CCTV; the need for accountability in the use of CCTV; privacy in public places and the home.

It is probable that some aspects of the use of CCTV equipment, and the management and release of information, do require statutory control.

PRELIMINARY

1. The Local Government Information Unit is an independent organisation to which 130 councils and the main relevant public sector trade unions are affiliated. In early 1996 the Unit produced a model code of practice for closed circuit television. The only attempt to address comprehensively the issues raised by the operation of CCTV, the code has since been taken by nearly 40 police forces and about 260 local authorities in the UK, as well as by other public and commercial organisations.

2. The model code was based upon research among local authority CCTV users, policy research conducted by the Unit, and the cooperation of a number of experts in the field, including representatives of the police, local government, and civil liberty organisations. The Data Protection Registrar was consulted throughout the preparation of the code.

3. The Unit has commissioned a research study of the usefulness of the code of practice, and the value of voluntary standards in the management of CCTV. This will proceed when funding is available. It is hoped that the research will enable substantive answers to be given on the need for statutory control of aspects of the use of CCTV and of recorded material.

4. The code addresses the use of all types of recorded material, anticipating that the current use of analogue based recording will within a number of years have given way to digital equipment. The Committee is urged not to ignore the issues raised by existing CCTV systems; accountability, and civil liberty concerns are among those issues which need consideration whether a CCTV system is digital or analogue. In this context it is important to note that analogue recordings are capable of being altered as are digital recordings.

5. The majority of existing CCTV systems in the public sector are believed to rely upon analogue recordings, and as a result are unregulated. It is important to note notwithstanding that data protection legislation may apply to the operation of any particular CCTV scheme, depending upon whether technological capacity and the intentions of the owners bring the scheme within the criteria of the 1984 Act. Forthcoming legislation which will implement the European Union Directive on Data Protection (95/46/EC) is expected to operate in a similar way.

*20 November 1997]**[Continued]*

RESPONSE TO QUESTIONS PUT BY THE SUB-COMMITTEE

Question 1

6. The first generation of digital based video recorders is now available in the market place. In general terms, computer based systems usually adopt some method of security, although no international standards exist and methods of protecting data vary in sophistication. The Courts have relied on the fact that analogue video material is usually continuous and is therefore complicated to tamper with, as each second of evidence consists of 50 individual pictures. Computer based or "snap-shot" capture systems store individual video fields (1/50sec). The Sub-Committee should be aware that increasingly video evidential material is being presented in Time Lapse Mode, in which individual snap-shot pictures of each camera are recorded at timed intervals of up to three seconds on the same video tape. The time lapse method is used by both analogue and digital recording systems, and is not continuous, or "real time".

7. The most immediate uses of digital technology in the development of CCTV include:

- image recognition systems—profiling using biometric measurement techniques;
- image enhancement products; and
- traffic surveillance systems which recognise the index numbers of vehicles, such as in the use in the City of London "ring of steel". Airports store a snap shot of the driver and car index number at car park entry and exit points to guard against attack or theft.

8. Also, in theory:

- post-production tools not normally available to the CCTV industry, but widely used in advertising and the film industry, could be used to edit video.

9. Anticipated is:

- profiling using algorithmic searching techniques to recognise individuals or groups.

10. An overall view is that technical barriers in the development of digital based video products have been broken. We can now expect substantial developments from manufacturing companies operating internationally.

11. The Sub-Committee is right to address the issues of picture origination, security and accountability of digitally produced video material before the impetus for technological development reaches a point that would make it harder to influence product design. Manufacturers of digital storage systems are reluctant to discuss what security measures they have designed in, nor do they appear cooperative at agreeing a universal standard between themselves.

12. If the intention is to use more information produced by electronic security systems as evidence in criminal proceedings, then the process by which it is gathered and stored must be fully understood, approved and audited such as would occur in a human system of investigation.

13. Manufacturers with new technology look for markets to sell based upon expected demand. They have less regard for non functional additions that do not add value to the product unless prescribed by law. In the instance of digital images and CCTV, it is probable that legislation will be required before safeguards will emerge which meet the standards required for the admission of evidence in legal proceedings.

Questions 2, 3 and 4

14. It is a commonly held assumption that a digital image can more easily be "doctored" than analogue. In fact, the development of post production techniques, mainly used in other markets, and the use of PC based programmes, opens this possibility for both analogue and digital material. Depending on the quality of the original analogue image, a TV frame can be converted to digital, edited, and converted back, without any trace. The real issue is therefore the availability of methods of protection, secure audit trails and reduction of the risk of tampering.

15. Current procedures for the protection of analogue recordings are reasonable: a video tape with many cameras recorded in a time multiplexed mode would all have the same date and time stamp, or other visual verifying features, all of which are recorded sequentially on tape. A single TV frame without other evidence or many successive and linked frames may not be reliable in evidence. A digital hard disk or DAT tape would store separate files which may not be laid down sequentially and therefore require an additional method of protection.

16. The Sub-Committee, in considering the use of digitally recorded material and single image analogue fields in evidence, should examine the need for safeguards. In our submission such material should only be used in evidence if a method of licensing or formal approval can be established which protects the recorded data from tampering. In our view there are two approaches that could be adopted, of which we prefer the first.

17. (i) To establish the performance criteria which must be achieved by manufacturers. It would be necessary in this approach to list generic measures which must be built into the security system. Generic

*20 November 1997]**[Continued]*

measures would include methods of encryption, embedded unique serial numbering, revision numbers, and hidden files preventing accidental deletion. Site codes could prevent a copied digital recording being replayed upon another system and allow non-interchangeability between personal computers and production systems. "Back-door" passwords would need to be protected. For material to be relied upon by the courts an independent method of approval, preferably by committee, of such measures would be required.

18. (ii) To define a sophisticated security system within each file which eliminates the ability of somebody to alter or copy data, using a form of encryption which the industry would accept while allowing for open competition. This approach would require manufacturers to develop an encryption system or protocol to approval stage. Approval would be given by an independently appointed technical committee. The difficulty with this approach is that the development of technology would outpace the legislation. There would be a danger that the requirements would be out of date by the time that legislation came into force.

19. The implementation of the changes that would be necessary to secure systems to a sufficient standard for the use of recorded material in evidence will only be developed if there is a requirement to comply with national law. Manufacturers such as those mentioned are receptive to the concerns of users, but are also subject to commercial pressures. The present systems that are in place do not reflect the technological standards that we would like to see, in part because manufacturers have no reason to make the commitment to develop the necessary security systems.

Question 5

20. If the issue of concern here is the security of data being transmitted, and further, of data connected solely with the presentation of evidence, then special problems will be raised. Briefly, this is because a system which allows for safe storage and recovery will not be secure if the link between two points of transfer can be tapped into, allowing material to be altered. In practice the complexity of such an intervention makes its occurrence unlikely, although possible. Substitution of a transmission will be possible. Concerns about associated risk will depend upon the context in which material is being used. Recorded material may be transferred as part of a security surveillance system, or as part of an investigation, and may not be intended for use in evidence.

Question 6

21. After pointing out that the cameras in Tiananmen Square were sold as advanced traffic control systems by Siemens Plessey, the writer of a working document produced for the STOA Panel of the European Parliament (1) observes: "Again democratic accountability is only the criterion which distinguishes a modern traffic control system from an advanced dissident capture technology."

22. The use of CCTV in public places does raise civil liberty issues in the UK. The tendency among those promoting CCTV to suggest that, "those who have done nothing wrong have nothing to fear", has contrasted with the attitude of those police and local authorities responsible for its introduction, who have looked for ways to recognise the interests of the individual and to establish standards for the operation of CCTV and the management of recorded material. The issues are not straightforward, and the successful implementation of effective measures is as yet uncertain, and is probably uneven. There appear to be five main civil liberty issues raised by the use of CCTV.

THE PROTECTION OF INFORMATION ABOUT INDIVIDUALS

23. The eight data protection principles indicate the issues to be addressed under this heading. The following are illustrations of how the principles were applied in the development of the Unit's model code.

24. The First Principle reads "The information contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully." In connection with CCTV, the concept of fair obtaining has been treated as meaning that it is important that individuals be aware that their image is being caught; that the identity of the owner of public systems be made known, and the purposes for which information obtained by systems will be used is made known. Published explanations should be complete and accurate.

25. Further data protection principles have been used to clarify the need to define the reasons for which recorded material should be retained and used, to require that observations and recordings be relevant and not excessive for the purpose, and to define the length of time for which recordings should be retained.

26. The Eighth Principle reads "Appropriate security measures shall be taken against unauthorised access to, alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data". Compliance with the Principle requires procedures and controls on access to and disclosure of data, management of data, and reliability of staff. These are highly relevant to the development of good practice for CCTV schemes.

20 November 1997][Continued

THE PUBLIC INTEREST IN THE USE OF CCTV

27. There is a balance between the concerns of the public with the prevention of crime, and the interest of the public in ensuring that CCTV systems are run according to recognisable standards. This includes the need for public consultation and information. The introduction of CCTV has relied upon the support of the public, and without this confidence the continued use of CCTV would be impossible. A Home Office report (2) in 1992 concluded that "public acceptance is based on limited, and partly inaccurate knowledge of the functions and capabilities of CCTV systems in public places". Unfortunately, it is believed that many of the consultation exercises that have been conducted have not been independent or fully informative. The importance of improved forms of consultation cannot be emphasised sufficiently when considering the pace of technological development.

ENFORCEMENT OF IDENTIFIED STANDARDS

28. The availability of an effective remedy is an integral aspect of individual civil liberty. Voluntary mechanisms for dealing with complaints or breaches of voluntary codes can seek to address this issue. Audit of records and recorded materials, training and supervision of staff, and accountability of the operators of systems to publicly accountable bodies are important aspects of the enforcement of identified standards.

ACCOUNTABILITY

29. In the introduction of CCTV police, local authorities, and other public bodies are working together in new ways. Such CCTV use often includes commercial interests. Many CCTV systems that cover places to which the public have access, or which overlook offices and homes, are run entirely by private commercial interests. Accountability in this context could be effected through a system of licensing.

PRIVACY IN PUBLIC PLACES AND THE HOME

30. Privacy in public places and the home is the most mentioned and least understood aspect of CCTV use. It is likely that domestic law will be applicable in the rarest of circumstances, but it is still important to recognise the relevance of Article 8 of the European Convention on Human Rights. Concepts of privacy may not apply as regards general surveillance in town centre schemes, although they may extend to instances of abuse by owners of systems. Surveillance of individuals in residential areas raises important issues, as do the circumstances of use and retention of recordings of individuals, wherever the recordings are generated.

Question 7

31. We consider that it is probable that some aspects of the use of CCTV equipment, and the management and release of information, do require statutory control. As explained, these matters are currently unregulated, unless an individual scheme falls within the data protection legislation, or unless covered by an effective voluntary code of practice. Statutory controls would need to be clear in imposing specific constraints, and avoid being prescriptive on the technological or operational solutions to be adopted. There may be a role for an approved code of practice. A system of licensing of schemes above a certain size may be appropriate. We consider that, should statutory controls be introduced, it is probable that there will remain a need for voluntary codes of practice to cover areas of activity that are associated with CCTV but not thought suitable for legislation.

32. Further research and consultation is required about the operation of existing voluntary standards to inform the process of developing legislation. The Unit is planning to examine the use of the model code of practice which it has promoted, to ascertain the position in terms of adoption and implementation, and to consider whether any changes are needed to improve implementation. The research will also set out and consider future options for both a statutory and voluntary approach.

20 November 1997]

[Continued

REFERENCES

(1) "An appraisal of technologies of political control", a working document for the Scientific and Technological Options Assessment Panel, European Parliament, Luxembourg, April 1997

(2) "Closed Circuit Television in Public Places", Honess & Charman, Police Research Group, Home Office 1992

Hilary Kitchin, Local Government Information Unit

Colin Greene, Principle, CMG Consultancy Advisor to the Unit

8 September 1997

Examination of Witnesses

MS HILARY KITCHIN and MR COLIN GREENE, Local Government Information Unit, called in and examined.

Chairman

142. Ms Kitchin, Mr Greene, thank you for coming to give evidence to us this morning and thank you also for the written evidence that you have kindly submitted to us and the other material, for which we are most grateful. For the record would you perhaps say who you are and, if you wish to say anything in the form of an opening statement, please do so?

(*Ms Kitchin*) My Lord Chairman, I am Hilary Kitchin and I am a policy officer at the Local Government Information Unit and I am happy that the point of view and the information I want the Committee to question me about this morning has been submitted. I am not going to make a formal presentation.

143. Mr Greene?

(*Mr Greene*) My Lord Chairman, my name is Colin Greene and I have been an independent security consultant for the last 18 years so I know the industry quite widely and this is an issue which is very dear to my heart because it is a question of protecting both public interests and being fair to the manufacturers and the customers and the users of systems in order to make sure that the courts can get material which can justifiably be used and is properly vetted and so on.

144. Thank you very much. In the main, Ms Kitchin, we will address the questions to you, but of course you will feel free to invite your colleague to reply when you judge that that is appropriate. May I start then with the first question. Can you tell us why the Local Government Information Unit code was really thought to be necessary and where did the prime concerns arise and, indeed, how great were they? Do you feel that those concerns have now been satisfactorily met and resolved?

(*Ms Kitchin*) My Lord Chairman, in 1993 local authorities were first being asked to commit large sums of public money to closed circuit television schemes in town centres and a number of local authorities that were affiliated to my organisation asked questions at our management committee meeting about the issues that they should be taking into account. They were very concerned that there was a lack of regulation and that they were being asked by individual members of the public about the civil liberty issues that were raised by closed circuit television, so I was asked by the organisation to do a review of the issues from the perspective of local government. The issues appeared much more

complex under that overview than they had initially. Civil liberty issues were raised in the sense of individual interest but also a number of issues of good practice from the point of view of local government about the management of systems and a whole question about the effectiveness of closed circuit television and whether it represented value for money. We had to make a decision as to which direction we went in and simply because of the range of issues that were raised and because we thought that regulation was something that we could address in a very practical way we decided to develop a code of practice. Initially it was intended for the use of our affiliates and we always expected it to have a wider application and to be made available more widely, but the project became much bigger than we originally thought. We found that not only did we have support from local authorities but we also had support from the police at a very senior level and the Association of Chief Police Officers were interested in being represented on the group of people who were advising us, and we brought together a wide ranging group in order to prepare the code of practice. Whether we are satisfied that the original concerns as far as regulation is concerned have been answered, this is something that we cannot yet say definitely yes or no to although we are aware that a large number of local authorities and police forces are using our code of practice; many have purchased it, and I regularly am contacted for advice about it and I have seen some examples of codes that have been drafted based on it. We always had in our mind the question of whether a voluntary code would answer all the concerns that our affiliates had raised and of course, until we have a better understanding of how the code is being used in practice we cannot be confident either that we have succeeded in answering everybody's concerns or that the voluntary standards are sufficient.

145. In your written evidence, Ms Kitchin, you talk about setting up a research project to look at that and make the point that when you wrote the submission funds were not available. Is that still the position? Do you have any forecast of when you may be able to do this work?

(*Ms Kitchin*) My Lord Chairman, we are hoping that we would be able to do the work next year, but we still have not got a sufficient commitment of funding.

Chairman] Thank you. Perhaps we could move on now.

20 November 1997]

MS HILARY KITCHIN AND MR COLIN GREENE

[Continued]

Lord Flowers

146. You have been dealing with a very large number of people, I presume, with a lot of different backgrounds and interests and so on. How easy was it to achieve the consensus that you evidently have achieved and what were the main differences of opinion and conflicts of interest maybe that you had to resolve?

(*Ms Kitchin*) My Lord Chairman, we found that by referring to the data protection legislation framework we were able to put forward a constructive and helpful way of thinking through the issues around the management and operation of closed circuit television and also the management of the material. Although in most of the schemes that are in place in the public sector at the moment the data protection legislation does not apply for technical reasons, or for reasons to do with the technology that is in use, nevertheless the principles are similar and we were aware that over a period of years it was quite possible that public sector closed circuit television would move toward a higher level of technology and would fall within the data protection legislation. Therefore, the concepts of fairness and good practice that were set out in the data protection principles and the guidance that had been issued under the Act gained support amongst the different interest groups that we brought together and it was possible for us to use that as a fairly solid foundation. We also had the advice of the Data Protection Registrar's office throughout the process and they helped us in an understanding of the application of the principles because, of course, the legislation is not aimed at closed circuit television; it is aimed at information on computer and processes on computers. There were some areas where we did have more complex questions to resolve. I can make a distinction in respect of those questions where we actually needed to explore the issues and reach a common understanding where perhaps there was not a common understanding at the beginning. One of those areas was accountability and the way in which local authorities, who were represented by our affiliates on the group, that was discussing the issues were concerned about the need to give an account of what they were doing, and then the different form of accountability to which the police are subject. We had to get an understanding of those differences. Then there was the question of recognition of individual interests and there, particularly in the voluntary code, it is hard to identify how you can protect individual interests and there we had to look at existing complaint systems, for example, and do an evaluation of how far we could import individual protection under the data protection legislation into a voluntary code. We also had to find practical ways of checking through monitoring, through audit and through evaluation which would satisfy everybody both in terms of effectiveness and in terms of the relevant cost. Therefore, we were balancing the local authorities' concerns about the processes, the police's concerns about the need to have security on the material and the interests of the civil liberty representatives that individual interests were taken into account.

147. That is very interesting. From what you say you have been working fairly closely with the Data Protection Registrar?

(*Ms Kitchin*) We have consulted them, my Lord Chairman, yes.

148. Has your experience with them led you to suppose that there might be some formal role that the Data Protection Registrar might play in your area, closed circuit television, and similar things?

(*Ms Kitchin*) My Lord Chairman, we certainly think that it is something that could be considered. The Data Protection Registrar, as I understand it, is able to approve a code of practice that is recognised in a particular area of an industry or even to formulate a code of practice and then take it into account in the procedures that follow under the data protection legislation. Of course, we have some questions about the ability of the Data Protection Registrar actually to initiate inquiries or initiate audit. As I understand it, the current powers are focused on or limited to where a complaint is made by an individual and, of course, it is still the situation that most schemes in the public sector at any rate are video—and, my Lord Chairman, I am sure that my colleague will be able to clarify any technical errors that I may make—but they do not fall within the legislation. Therefore, I think that that is an option for the future rather than for us to deal with currently.

Lord Brain

149. If I may just raise a question on this, my Lord Chairman, before we move on, you have been talking here about local government. Are most of these schemes operated by a department within a local government function or are they subcontracted to professional, probably commercial, contractors to run the schemes generally?

(*Mr Greene*) My Lord Chairman, the answer is a mixture of both approaches. Well run local authorities generally manage their own systems, but there are equally some town centre schemes which are run by independent monitoring services. There are nationally approved standards for operators which are now coming into place, so there are some qualifications which you can apply to the operators who run these systems. Equally, however, there is a large private sector which is not managed at all, and I am including, for instance, shopping malls, perhaps railway stations, although some do follow certain operational guidelines or codes of practice.

150. No, I was talking about local authorities specifically. The question was about local government.

(*Mr Greene*) I think that the answer is a mixture of both approaches.

Lord Brain] We are well aware of the other ones and I do not think that we need to pursue that red herring at the moment.

Chairman

151. While we are on this sort of matter, in your written evidence you mentioned that there are 130 councils in the relevant public sector trade unions that are affiliated to you. Can you just clarify whether that covers the whole of the United Kingdom and Northern Ireland or is it not as complete as that?

20 November 1997]

MS HILARY KITCHIN AND MR COLIN GREENE

[Continued]

Chairman *contd.*]

(*Ms Kitchin*) My Lord Chairman, the local authority affiliates are in the main part in England and Wales and we have had in the past—and I think we do have at the moment—a small number of Scottish authorities who are affiliated. The trade unions again cover England and Wales although we do have some connections with organisations in at least one organisation in Northern Ireland.

152. So it is fair to conclude from that that those who take an interest in your code of practice from their association do not represent a complete coverage of the United Kingdom and Northern Ireland?

(*Ms Kitchin*) Well, my Lord Chairman, that is a different question because we consulted and we promoted the code of practice more widely than that and, in fact, those local authorities and police authorities that have taken copies of the code extend throughout the United Kingdom.

153. So there are no gaps, in other words?

(*Ms Kitchin*) There are gaps of authorities and police forces that have not taken a copy, but police forces in Scotland, Wales and Northern Ireland, England and, I think, at least one of the Channel Islands have taken it. As far as local authorities are concerned, I have not done an analysis of the difference on a country by country basis, but it is comprehensive and we have promoted it widely and we ran a briefing conference for local authorities and the police on the code in Glasgow, for example.

154. Would you be good enough perhaps to let us have a written note of the coverage, just in terms of a statistical percentage, so that one has some sort of feel for the work not only for those who are members but also for those who have taken an interest in or who have taken up the code?

(*Ms Kitchin*) I will certainly address that, my Lord Chairman.

Baroness Hogg

155. Amongst those who have, have you had feedback as to why they have not adopted the code? Is it just that they have not got round to it or have you had feedback that might indicate something that some of them do not like about the code, that they found it missing certain areas and so on, or have you had no negative feedback?

(*Ms Kitchin*) My Lord Chairman, what little feedback we have had suggests that, for example, local authorities in Scotland have some questions about the different law that applies in Scotland and we tried to address that in the code and explain how it could be adapted into a different criminal jurisdiction, but I assume that that is a reservation as far as Scotland is concerned. However, as far as any other feedback is concerned, my Lord Chairman, no, I have not had any negative feedback. One element of the research that we would want done is examining how successful the code had been for those who had taken it, but perhaps also including a group of authorities or police forces that had not taken it.

156. If I may move on now to the issue of public awareness, I am interested that you mention that there is limited public knowledge and lack of

awareness of closed circuit television systems. I am not quite sure of the extent to which that means that there is limited knowledge of how they work and who is operating them or their actual presence and the surveillance purposes for which they are being used. I wondered what your view is of the extent to which this indicates an implicit acceptance of these schemes and what might trigger a loss of confidence. It is a difficult balance, is it not? As you were discussing different operators a moment ago, it came into my mind that it might be appropriate, for example, for it to be apparent on schemes who was operating them, the brand or whatever. On the other hand, that would make the schemes much more visible possibly in rather an aggressive way and that might tip the balance of acceptance against them. I do not know what your views are on this bundle of issues?

(*Ms Kitchin*) My Lord Chairman, firstly, as far as public information is concerned certainly there is work going on at the moment. For example, the British Council of Shopping Centres have just recommended a sign and our code recommends a sign which complies with the data protection framework which suggests that the organisation responsible for the closed circuit television scheme should be identified, and it does appear probable that a sign could be identified which is either neutral or reassuring rather than appearing threatening and suggesting that this is an area which—

157. Like Big Brother plc?

(*Ms Kitchin*) Yes, or that this is a high crime area. As far as public knowledge is concerned, my Lord Chairman, it does seem looking at it in a very broad way that people do accept the presence of closed circuit television. I think that our concern is that once you ask more detailed questions than a simple routine two or three questions of a simple survey in a shopping centre, for example, once you give people the opportunity to ask for information and answer their questions, more concern arises over who is behind the camera, whether it is actually to protect, and the research that was carried out and published by the Home Office in 1992, to which I refer in our written evidence, did suggest that once people were given the opportunity to ask questions and had more information, a greater proportion of them expressed some concern.

158. The other thing is, may I just pick you up on the kind of concern that is being expressed. You said that questions came up as to whether the system actually protected. Are the questions of concern, therefore, if you like, about the effectiveness of the protection or are they about the intrusion into the privacy of the individual? Which—and this is not to say that they could not be concerned about both—is the balance of questioning?

(*Ms Kitchin*) It is hard to answer that from memory, my Lord Chairman. What I can do is to provide a copy of the report to the Committee, if that would assist.

Chairman] Thank you very much for that.

20 November 1997]

MS HILARY KITCHIN AND MR COLIN GREENE

[Continued

Lord Carmichael of Kelvingrove

159. If I may just follow on on the question of individual privacy, have the public any say or have you had any protest about the siting of the apparatus because you could have apparatus—a shopping mall is a different thing, it is a public place—peripherally close to someone's front door and they may feel that every movement they made was followed. Could they have any say in asking you to move your cameras? Have you had any complaints in that way at all?

(*Ms Kitchen*) My Lord Chairman, we do not receive individual complaints. What we do hear, however, is the concerns of people in local areas expressed through our local authority affiliates and just that question, that range of issues, was raised as we were drafting the code of practice. Unfortunately, we had to rely upon our affiliates' understanding of the problems that they had in discussing the introduction of closed circuit television in residential areas and our own level of research on questions of privacy in order to begin to address the issues. We saw that the section of the code of practice that dealt with closed circuit television in residential areas was very much a beginning of a process of addressing those concerns. Since the code was published at least one research project has been set up to look at the way in which people who have closed circuit television in their residential area do respond to it and do feel about it and do express levels of concern. I think that is something that is going to feed back into developing an ultimate national code of practice.

Chairman

160. Yes, Mr Greene?

(*Mr Greene*) My Lord Chairman, may I just add some riders to the comments that have already been made. I think that collectively one of the concerns that the working party had in producing the code of practice was the unregulated nature of many control systems, the selection of staff, and while many local authorities had the will or perhaps the initial confidence to write a code of practice and put it into effect there was no legislative requirement to do so, so our indications both from consultants working in the field and from the Local Government Information Unit were that many of the codes were not being followed. There are still concerns, for instance, about the release of video tape material to the public media without the knowledge or consent of those involved. There is therefore a whole series of issues related to public confidence in the operation of schemes. Public confidence in closed circuit television is a perception which has not been fully measured yet and support could collapse very quickly if an incident occurred which resulted in or proved that there was negligence on the part of operators or the owners of schemes. Whether a scheme is in the public sector or in the private sector is irrelevant as far as good practice is concerned; we are looking at a wider issue. There is so much closed circuit television in existence that until there is some requirement to follow a code of practice there is going to be unchecked availability

of material and where that occurs, that is really our major concern.¹

Lord Phillips of Ellesmere

161. My Lord Chairman, may I just broaden the question a little. I am sorry if I have missed it in the code of practice, but were you at all concerned about the quality of the equipment that is installed, the resolution that is attained in the images, and the concern that there might be about enhancement of images when they became important in criminal or civil cases?

(*Ms Kitchen*) My Lord Chairman, we were aware that the Police Scientific Development Branch and others have been developing technical standards to a very high level, and we decided to focus on the operation and management in establishing schemes, but we have kept abreast of developments in that direction. However, we thought that it was not appropriate to include in our code, though we do refer out to other standards, parallel standards that are being developed.

Lord Kirkwood

162. Just briefly about the code of practice, my Lord Chairman, did you consider or give recommendations as to the storage, the life time of information stored in this way, where the tapes are re-used every 36 hours or whatever it may be and there is a limited time in which that information is stored? Did you consider things like that?

(*Ms Kitchen*) Yes, my Lord Chairman, we did. The conclusion that we reached, doing a review of the research project that we had done and the experience of the people who are in our advisory group, was that we put a period of 30 or 31 days on retention of recorded material unless it was abstracted for evidential purposes.

163. But normal is a month?

(*Ms Kitchen*) Yes, my Lord Chairman.

Chairman

164. If we may move on now to question number four, we have already dealt with this in part, I think, but I would like to press you, if I may. This is dealing with whether or not there should be a legally enforceable code, and I rather read into what you have already written ahead of the research, and following on from what Mr Greene has been saying to us, that you have a feeling that some more legally enforceable arrangements are required? Are there any other points that you would like to give to the Committee which help to reinforce that perception about ideas of the flouting of the code? Again, Mr Greene may be able to help on this. Could either of

¹Footnote by witness: The LGIU was concerned that in the period during which the model code of practice was being developed, the development of codes of practice in the field had not kept pace with the speed of the introduction of CCTV. There was also concern, expressed anecdotally, that existing codes were not fully complied with. It is the LGIU's view that further investigation is needed before conclusions can be drawn on compliance with codes drawn up under the model code of practice.

20 November 1997]

MS HILARY KITCHIN AND MR COLIN GREENE

[Continued]

Chairman *contd.*]

you perhaps just add to that it would be very helpful to the Committee.

(*Ms Kitchin*) My Lord Chairman, there are some examples, not of the flouting of the LGIU's code, but of what we would see as breaches of good practice in some instances where there was an existing code of practice which have been reported in the press. One is of disclosure to the media of recorded material showing a man who had attempted suicide and who had in fact been rescued as a result of the intervention from cameras, but the material was then disclosed without his permission to local media and national television which caused him considerable distress. There was also the prosecution of a camera operator in south Wales who was using the observations that he made on camera to follow young women and then make a telephone call to a telephone box, and he admitted offences in connection with that. Clearly it had been happening over a considerable period of time. Then there is also a report in the London press of a rail operator which was relying on a local minicab firm to watch its cameras out of office hours at night. Therefore, there are examples, but I think that the main arguments that we have for the need for increased regulation either relate to the nature of the voluntary code or relate to the public policy issues associated with the scale of the use of closed circuit television. If I may deal with the first, my Lord Chairman, the limits of voluntary control are that they have no bite, there is no enforcement unless the owner of the scheme is willing and puts in considerable effort. The scale of closed circuit television and the sheer volume of recorded material suggests that a public policy approach ought to be taken, and that would lead to a belief that there should be more than voluntary regulation. We are also concerned about the private sector and the increasing development of closed circuit television on quite a large scale by commercial or other private interests and how in the long term these are expected to link into public sector schemes as partnerships are established, for example, or that there will be links in other ways through the police having electronic links, for instance, or security companies having electronic links. Therefore, the potential increase in scale also suggests that there are some elements of the management and operation and use of material that should be put on a stronger basis.

165. One of the difficulties with that might be that some of the material that is released and, for example, used by the media is seen as helpful, drivers behaviour on the roads, you know, one is for ever getting programmes showing what stupid things people get up to, and that has been captured by closed circuit television or police cameras. Now in respect of those sorts of things in the way that you are looking at it should they not be covered by legislation and restriction that we are talking about, is it a matter of common sense or how would you approach that problem?

(*Ms Kitchin*) First of all, my Lord Chairman, I think that there are different opinions on the educative or information role that the disclosure through the media has. We have amongst our affiliates, including the former chair of the organisation, those who very strongly take the view

that if the local authority wanted to establish the credentials of its scheme and establish confidence in its scheme locally there were means of doing that through public information methods, through provision of information about the success of the scheme in obtaining successful investigation and conviction that would succeed without the need to disclose large amount of material to the media where it has a very high entertainment value and has a potential commercial value, so we do have reservations about that and we would want to see in any eventual regulation the right balance struck there.

166. Mr Greene, you wish to come in?

(*Mr Greene*) My Lord Chairman, we believe that there is nothing in the LGIU code of practice that any authority that is currently developing rules of good practice would have any difficulty in abiding with and running with. Local authorities or private companies who were simply window dressing by installing television systems as a front would have difficulty in conforming to the code because their schemes would not comply with good practice. I believe there is a consensus, from the acceptance of the report, that all the material there in fact could form the basis of an extended code of practice to cover the use and dispersion of closed circuit television. There is nothing there that anyone would have difficulty with in the normal running of a system at all. I think really that I have summed it up, thank you, my Lord Chairman.

Lord Ackner

167. You have emphasised that the code is voluntary and that there is no legal requirement to abide by it. How would you envisage imposing such a requirement? Would you do it via a licensing situation or what would you have in mind as the means of bringing home the legal obligations which you want to see mirrored in the code?

(*Ms Kitchin*) My Lord Chairman, if I may answer that, we have already mentioned that we have been considering whether a code of practice could become part of the tools of the Data Protection Registrar, but we also have considered the possibility that the code could be given status through the Secretary of State being given power to issue a code in primary legislation, and then the code itself would be issued in the way that statutory codes are in other and perhaps related fields. The development of the code could be based on consultation and could meet the agreed perception of the issues that had to be addressed and the technological status of closed circuit television systems at that point and could then be re-visited and amended without having to go back to parliament and having to return to the need for primary legislation.

168. Do you envisage a licensing process that you cannot mount these cameras that look into public areas without a licence?

(*Ms Kitchin*) My Lord Chairman, it would be a very efficient and locally accountable way of checking on and maintaining checks on compliance with a code of practice to have a system of licensing that was based on the local authority. This could

20 November 1997]

MS HILARY KITCHIN AND MR COLIN GREENE

[Continued]

Lord Ackner *contd.*]

cover closed circuit television systems according to criteria that stayed within the range of perceived risk. Licensing would not necessarily apply to the local newsagent and the high street shop with maybe one or two internal cameras but that it would catch much larger retailers or larger industrial use cameras which covered areas to which the public had access or would catch the scheme in the railway station or other public building.

169. Do you see any difficulty in drawing a line in that field?

(*Ms Kitchen*) My Lord Chairman, I think that there would not be insuperable obstacles to defining an appropriate field. I had originally thought that it could be done by the number of cameras that any individual organisation had, although Mr Greene has pointed out to me that there might be difficulty there depending on, let us say, the number of cameras that were in use at a railway station. It might be a very small number and they would then be outside the scheme. The steps that would have to be taken I think would be to identify the perceived risk and then have caught within the licensing system those schemes that did bring with them a perceived risk if there was a lack of effective control. One would therefore have licensed, for example, schemes that were linked into the public scheme or that had links to other nationally based closed circuit television systems that were run by a major retailer, for example.

(*Mr Greene*) My Lord Chairman, I think that we are collectively concerned that self regulation would not work, because there is no bite in current legislation to enforce compliance. Whereas, for instance, energy efficiency schemes, there is a financial interest in performing and meeting targets, so a licensing system would allow schemes to be registered without having to develop a very complex legislative procedure. We need a vehicle by which to license systems and perhaps—it is only a suggestion—the Data Protection Registrar may have the opportunity of including that because of their well-developed database, but they would need to be consulted, of course, and answer themselves. We are also concerned that the code sees a wider audience, that we involve institutions, commerce, education, hospitals, in areas where cameras are used publicly because much of the evidence that has been produced to the courts comes from the private sector, not just the local authority. It is in our interests collectively to have a uniform system which embodies good practice. For example, the PSDB's primary concern has been since the day they started to focus on the quality of pictures. All their programmes are written around effective closed circuit television schemes based on the clarity and the size of image. Those values can be inserted in a code of practice as well. Therefore, a code of practice, as we have outlined, could join together different areas of interest both from a justice point of view and from the public interest point of view. Manufacturers, because I think that there is an interest there, should be consulted so that they are actually producing products that meet the requirements of a code of practice, particularly when you look at the digital argument which we will discuss later. We believe

therefore that there needs to be a group that can co-ordinate the input from different areas because the code of practice is really part of an operational manual; it is not the only requirement.

170. But you would include the small shop?

(*Mr Greene*) No, my Lord Chairman, I think that you could exclude certain areas. For example, the small shop that we may define as the corner shop does not really have a public interest argument to answer, so they would fall outside that guideline. You could perhaps measure by turnover or by number of employees. However, where there are areas that the public have access to, shopping malls, railway stations, education, hospitals and so on, then there is a need to embody those groups within a code of practice in a licensing system.

Chairman] Thank you, that is very helpful.

Lord Brain

171. My Lord Chairman, I think that Mr Greene has largely answered my first question but I have a second question that has come from what he has said. If I may just pick up the first point about how you define the area that requires cameras to be licensed, you used the word shopping mall which very often is directly adjacent to a public street and the public very often do not realise which is which. You then go to some of these big open plan stores which have shops within a shop and things like that down, as you say, right to the corner shop. I wondered whether it was, first, a matter of area and, secondly, a matter of the number of people who do actually make access to one of these places that might be considered?²

(*Mr Greene*) My Lord Chairman, I would suggest that an appendix to which you can then add and which you can amend would be a very useful way of developing the criteria. For instance, in the shopping mall criterion you could define multi-tenancy as a criterion, so where there is more than one company operating within an enclosed building I would believe that they should fall under the code of practice, but where you are looking at a single store in a single building, internally they may not fall into the code of practice because it is private property: you go in there to shop of your own freewill. Where there is a public thoroughfare that joins two or more department stores, whether it is covered or not, I think that should fall under a code of practice. Therefore, there needs to be, I agree with you, a clear distinction that the public understand between what is public and what is private, and I think that that can be done within a document.

²*Footnote by witness:* This circumstance, of the public and commercial sector developing different approaches to the introduction of safeguards, could lead to an anomaly, in which large schemes wholly in the commercial sector are not subject to appropriate controls. It may be that commercial schemes will be covered by the general framework of data protection legislation. Nonetheless there does need to be an examination of the general criteria which could be applied leading to compliance with a national code of practice, and an assessment of how far such criteria would overlap with public expectations about the management of CCTV, on their premises, by companies in the commercial sector.

20 November 1997]

MS HILARY KITCHIN AND MR COLIN GREENE

[Continued]

Lord Brain *contd.*]

172. Thank you. Now if I may come back to the other point, a point was made earlier, my Lord Chairman, where I think I understood the evidence to be that at the moment most closed circuit television operations are run on a video tape system of recording. This does not mean to say that they are not digital, because it is digital information that is put on to tape, but I got the impression from what Mr Greene just said that in the future there is going to be much more going direct into computer and stored in computer disk form and things like that. Is this safe, and would it be more likely that the Data Protection Registrar would take an interest if it was on a computer disk type operation rather than the video tape operation as at the present time? Have I stymied you?

(Mr Greene) My Lord Chairman, the digital argument, as I have said in my precis, is a very complex one because, as you rightly said, analogue tapes can comprise of both digital information and analogue material although recorded on an analogue machine. Currently there is a perception that digital is far easier to tamper with than the existing analogue recording media, which is not true. Anyone with the right technology can tamper with an analogue tape and present it as evidence. Our concern therefore is that all recording systems should be embraced by some kind of requirement to protect the information at source. Having given a lot of consideration to this point, we believe that it has to fall on the origin of the material. We suggest that in your recommendations you give a higher priority to protecting the originality of material because I do not believe as a technician that you can put hand on heart and say that any watermarking or serial numbering is foolproof. Through time, codes could be broken. What you can do, however, is try to strengthen the security of material, so where it is recorded should remain very tightly secured and the material should be logged so that there is a written record that could not be changed giving details of recording, use, access, and so on. The use of digital technology, my Lord Chairman, I think will certainly increase because the cost is coming down and the ability to store more material is fast exceeding what it was even on a monthly basis. From a quality aspect digital is much better because you can record and store higher quality material without interference or noise. So clear picture evidence can be produced both to eliminate a suspect as well as to convict them. However, there are concerns in my quarter that manufacturers are not working to the same agenda. They produce products based on a market evaluation of need and their designs do not necessarily reflect the public interest argument from day one. They will only modify this approach if a committee like yourselves produces a directive which says: for products to be used for recording of potential evidential material it should follow this quality aspect or good practice procedure. Stating the minimum requirements that should be adopted so that the material source is reasonably secure and has not been tampered with. That is an area where I see great problems at the moment because there is no harnessing of manufacturers' interests and driving them down a route which could secure a common and collective solution. The longer the time scale the

more difficult that will become. The example, if I may quote you this, is the difference between Betamax and VHS tape. As a European country, we are familiar with domestic VHS tape, but in America Betamax is the dominant format. All around the world you will find different countries that have majored on one standard or the other—the reason is purely a marketing achievement. In fact, the Betamax is probably of better quality, but the reason that we do not have it is because VHS was marketed more strongly in the start. Manufacturers will take a lead by penetrating markets much earlier and achieve a market share and exclusivity which it would be difficult to break. In context, CCTV products would then be installed without controls or guidelines being put in place, so then you are working in a reactive sense, which I think is far more difficult to solve. I have probably said enough, my Lord Chairman.

173. If I may, my Lord Chairman, I was just going to pick up one point. I think that you are saying, Mr Greene, but I would like it on the evidence, are you really saying that the manufacturers ought to be made to instal a read-only type device, perhaps a CD disk or something, and would the software that is feeding that disk indicate at regular intervals date and time or something like that so that as it is read you can get this information and know that it has been running consecutively? Were you saying that really it is a question of writing the right software?

(Mr Greene) My Lord Chairman, I think that it is a matter of designing controls. I am not qualified to answer specifically whether it should be a watermarking or serial numbered. The principle I suggest is that the product that produced the material should have some unique serial numbering system which identifies it only with that particular recording and that that recording, if removed and replayed or edited on another machine, could not be stored in its original form. The concept therefore is that once that material comes out of that machine and is "used" on something else it cannot be stored in its original form, and so it would be clear that the evidence had been changed.

Chairman

174. There is just one point, to go back to what you have been saying earlier, all of which has been very interesting. We are talking about an audit trail. Did I understand you to say that you still believe, talking about using this material evidentially, a paper audit trail will be an essential part of the proof of the validity of the material being presented as evidence?

(Mr Greene) My Lord Chairman, these are arguments which we have not had a lot of discussion over. It is part of the system, making the owners of schemes accountable for their actions to the courts. One example that we discussed recently was that if a scheme is licensed the owner is required to declare the type of technology and how it is used. At a later stage material from that site then presented in court defence for instance, could question the validity of the original licensing and if there were sufficient grounds to say that that scheme had not been run properly, they could question the value of the material being presented. Both the police and the

20 November 1997]

MS HILARY KITCHIN AND MR COLIN GREENE

[Continued]

Chairman *contd.*]

owners, therefore, would have a vested interest to make sure that they uphold the highest standards possible and be encouraged to have audits carried out annually, if not part of a licensing scheme. On that basis, my Lord Chairman, that is a system that the public can understand. My concern would be that persuading the public on the basis of technological argument is far more difficult. As people have already said in other papers and in public statements, once you get experts in court, then the technical argument becomes very complex. The jury must decide on the rights and the wrongs and the validity of the material that is being presented by two professionals with directly opposed opinions. I think that that is something one should try to avoid.

Lord Phillips of Ellesmere

175. You seemed to be saying earlier on, Mr Greene, that you thought that the quality of the original recording could be such that enhancement could become in a sense an illegal operation. Did I get you right on that?

(*Mr Greene*) No, my Lord Chairman, in fact I did not suggest that. The police have developed "improvements" to software which I think is an excellent way of traceability in improving the quality of poor images, and I have confidence in that scheme. I would have less confidence in the commercial sector operating enhancement schemes. I think that collectively we much prefer to drive the argument back to the originality of the material and securing that that is of the original concept and, if enhancement is made, there is a traceability attached to it. Already there are many systems on the market operating on different performance criteria, so I think that it is going to be very difficult to have a single test that you can apply to all systems to verify validity and traceability.³

Chairman] I think that we should now move on.

Lord Kirkwood

176. My Lord Chairman, I would like to ask a question about democratic accountability over the control of closed circuit television systems which you mention in your memorandum. What sort of body would you like to see put in place to maintain the code of practice?

(*Ms Kitchin*) My Lord Chairman, I think that the system that we have described so far suggested a system of licensing through a local authority and establishing a code of practice through consultation, either through a statutory process presumably based on the Home Office or through a recognised code administered through the process of the Data Protection Registrar. Yet in terms of thinking about the difficulties of reconciling the wide range of interests that are involved here and the difficulty in establishing a completely new structure and completely new system of recognition, yet also seeing

the necessity to take the work we have already done further, it may emerge that the framework which I have described is insufficient.

177. But you do not envisage setting up a new body? You are taking systems that exist at the moment?

(*Ms Kitchin*) No, that is correct.

Lord Carmichael of Kelvingrove

178. Could you give us any idea of a local authority requiring specialised staff for this sort of work and what the effectiveness of cost benefit would be to the local authority? Are there any barriers, have you come across barriers of local authorities balking at the cost?

(*Ms Kitchin*) My Lord Chairman, one of the issues that we had to resolve when we were drafting the code of practice was the cost of setting the standard for the selection and training of staff and there are schemes being developed to establish recognised training for staff who are responsible for closed circuit television operation. Those are recognised by the industry. What we sought to do was to encourage local authorities to employ staff who had some form of training or to provide that form of training in post and to adopt a process which over a period of time would lead them towards establishing the best standard rather than saying that all local authority schemes should comply with the best standard at the beginning. That was partly because of the question of cost and it was partly because of the question of lack of existing satisfactory training and the lack of existing qualified staff. As you appreciate, my Lord Chairman, closed circuit television is expanding very quickly. In the research that we did we found that there was a very mixed use of staff and some schemes do employ well qualified staff or provide training and employ a high level and a high number of staff for the operation of their schemes. Others often employ a much smaller number of staff and they do not provide the same level of training. It is one of the situations that our code of practice has sought to address and it is being addressed by other organisations with an interest in closed circuit television.

Chairman] Thank you. We will have one final question from Baroness Hogg.

Baroness Hogg

179. I am a little concerned about where some of these approaches might lead. To move from a position where you are in a sense a facilitator, thereby producing a very useful code of practice, to local government taking on the licensing responsibility where they would therefore implicitly be responsible for how all schemes were operated, there is a spectrum here of expense that could get very high indeed and you could end up with a huge local government bureaucracy checking the operation of all these schemes on an extremely frequent basis, given the ability of the systems either to malfunction or to be run inappropriately. I am not sure whether you are thinking of stopping with local government or whether you are considering penetrating into

³Footnote by witness: The point here is that the development of methods of traceability is in its infancy. The opportunity exists, therefore, to intervene and establish standards. Any difficulties will arise from the present situation of there being many systems on the market.

20 November 1997]

MS HILARY KITCHIN AND MR COLIN GREENE

[Continued]

Baroness Hogg *contd.*]

areas of public authorities and their systems with your licensing schemes or, indeed, into the private sector. I have to say, my Lord Chairman, that my inclination would be to look if one could not land this responsibility very firmly on some kind of trade association, leaving the users of such schemes and such firms such as yourselves to say that you will not employ those who do not confirm to a code of practice put in place by the trade association that you consider satisfactory. I wondered whether you might have any comments on that?

(*Ms Kitchin*) My Lord Chairman, the question of cost is certainly important and while the proposals were being worked out one of the issues that would have to be addressed is how the balance of risk that was perceived and the number of closed circuit television schemes that might be brought within licensing balanced against the cost of having a system of licensing. The perception that we have in proposing that local authorities be responsible for local licensing inspection is not in increasing the extent of responsibility but with the knowledge that local authorities have an existing licensing review responsibility in other areas.⁴

180. And big bills in other areas. You have only got to think of any licensing authority and the kind of expense that they have to undertake if that licensing role is to be taken seriously as somewhere or other the legal system will ensure it is.

(*Ms Kitchin*) I do agree that the question of cost has to be addressed. The important thing about its being based with the local authority is that it is in the local area and the local authority can answer questions of local people about the schemes in the locality and be responsible for the administration of the supervision of the use of closed circuit television in the locality, particularly if those schemes are linked into the local authority scheme in some way. I think that if the question of cost did prove to be

prohibitive, my Lord Chairman, then I would agree that in parallel one would have to be considering the possibility of other forms of inspection. I am not excluding that, but for the question of local responsibility and accountability we would prefer it to be based in the local authority area, if it could.

181. My Lord Chairman, I do not want to take up the Committee's time by pressing this any further, but I am still a little worried, because unless you force trade associations to take these responsibilities seriously you will slide into the local authority having responsibility with all the costs involved, and that is then very difficult to dismantle.

(*Mr Greene*) My Lord Chairman, we have an institution called SITO which is involved in writing technical and operational standards. They also operate courses for inspectorates, so they could take on the task of training up individuals, even in the private sector. Alarm and CCTV installing companies could also assess schemes. Where we would be slightly concerned is where local authorities were self-assessing each other. We do not feel that that would work. Commercially I believe that they would get good value for money. A scheme could be vetted and a report made for perhaps several hundred pounds, £500 or £600, which annually would not be a considerable sum of money.

Chairman

182. Ms Kitchin, Mr Greene, I am afraid that the clock has beaten us, but thank you both very much indeed for being very helpful with your answers to our questions this morning. Are there any burning issues which we have not touched on which you would like to raise?

(*Ms Kitchin*) No, thank you, my Lord Chairman.

(*Mr Greene*) Thank you, no.

Chairman] Thank you very much.

Memorandum by Mr Alan Shipman

LEGAL ADMISSIBILITY OF ELECTRONIC DOCUMENTS

A BRITISH STANDARDS INSTITUTION CODE OF PRACTICE

WHAT IS THE CODE?

The issue of the legal admissibility of electronic documents has been long outstanding, and the subject of many discussions and articles. Expert legal opinion suggests that the issues are best resolved by the creation and implementation of rules of "best practice".

In 1993, an open meeting was held at Cranfield University to explore these issues. The result of the meeting was the formation of the Legal Images Initiative (LII), which subsequently developed a set of management principles, around which a statement of "best practice" could be built. These are now being published by BSI as BSI-DISC PD0010.

In parallel to this work, a group of vendors and users under the auspices of the Document Management Suppliers Group (now the Document Management Forum) developed a set of criteria to be used in the development and use of electronic document management systems, such that they could be operated within the rules of "best practice".

In 1994, the Standards Committee of UKAIIM agreed to work with the LII and DMSG, to produce a document that the British Standards Institution could publish as a Code of Practice, as an authoritative

20 November 1997][Continued

statement of “best practice”. This work concluded with the publication of BSI DISC PD0008 in February 1996.

Throughout the development of the Code, wide ranging support was received from industry, from systems suppliers, users and the legal fraternity. This support has continued after publication, with over 3,000 copies of the Code being purchased, and over 1,000 people attending various seminars organised by LII and BSI. Not least was the support of Sir Kenneth Warren (past Chair of the Parliamentary Select Committee on Trade and Industry) and The Right Honourable Lord Justice Saville at the LII launch seminar.

OBJECTIVES OF THE CODE

The major influence in the development of the Code of Practice was the commercial desire to destroy original documents, and rely upon the electronic versions for use in court cases when necessary. To this aim, the Code contains requirements for the Document Management System itself (hardware and software), and recommendations for the operational procedures implemented by the users of the System.

Often, documents are stored for a considerable length of time on such systems. To be able to claim conformance to the Code, it must be in place (and be seen to be in place) for the whole storage life of the document.

HOW IS IT IMPLEMENTED?

Many users of Document Management Systems will be familiar with the implementations of Quality Systems, such as ISO 9000. These implementations take a great deal of time and expense, and require the use of external annual assessors for certification. The Code of Practice does not work in this way.

BSI have also published a “Compliance Workbook” (BSI-DISC PD0009), which in conjunction with the Code of Practice, facilitates self implementation and certification. Resource will be needed for this, but such resource should be cost effective as it is likely to lead to a well run Document Management System.

VOLUNTARY OR MANDATORY?

The Code of Practice has been developed as a voluntary Code. There is no necessity to implement the Code. The fact that the Code has not been implemented will not stop electronic documents being admitted as evidence to a court of law.

However, the Code details what industry agree are the best practices for the management of electronic document management systems. If a system does not operate to these “best practices”, then it is not unreasonable to suspect that it is not being well run. This allows an opposing side in a legal case to question the authenticity of the electronic images, and put the onus firmly on the presenter of the electronic documents to defend their system, and give good reasons why they have not implemented the Code.

WHY SHOULD IT BE IMPLEMENTED?

As can be seen above, implementation of the requirements of the Code of Practice for Legal Admissibility of Information Stored on Electronic Document Management Systems (BSI DISC PD0008) will ensure that a Document Management System is being run to “best practice”. This will increase the confidence with documents stored on the system, and should enable them to be used with the same (or possibly increased) authority as the original documents.

Why increased authority? With the common availability of “scanning” photocopiers, seamless manipulation of paper documents is becoming common practice. So, can any such documents be used with total confidence? A properly managed Document Management System does not allow such manipulation to take place. It may be that, in a short space of time, an electronic image from a Document Management System conforming to the Code of Practice will be perceived to be better than an original paper document!

CONCLUSION

If you are intending to use a Document Management System, and anticipate that electronic images will be needed as evidence in a court of law, implement the Code of Practice as soon as possible.

Alan Shipman—Group 5 Training Limited, Chairman—UKAIIIM Standards Committee, Editor of the BSI Code of Practice.

*20 November 1997]**[Continued]***Memorandum by Mr Alan Stevens****STANDARDISATION****1. STANDARDS AND REGULATIONS**

Standardisation is a very broad concept that includes both the creation of consensus-based documents by recognised bodies and the voluntary use of these documents as standards for collective benefit.

Standards do not in themselves impose any obligations of adherence. Regulations, which the law requires to be implemented, may however refer to standards in such a way as to make compliance with them compulsory.

2. TYPES OF STANDARDS

Standards are prepared for various reasons and many uses. To this end, there are different types of standards such as vocabularies, methods, specifications and codes of practice, guides or recommendations. An important distinction is drawn between a specification (that prescribes requirements to be fulfilled) and a code of practice (comprising guidance and recommendations to be followed).

The contents of any type of standard can be subdivided into normative (ie standardising) elements and other elements which are purely informative, and are distinguished by context and wording.

3. UK GOVERNMENT AND BSI

A Memorandum of Understanding between the United Kingdom Government and the British Standards Institution on standards first agreed on 24 November 1982 was most recently updated on 27 July 1995.

4. DISC AND BSI

The acronym DISC derives from Delivering Information Solutions to Customers through international standardisation.

DISC is the department within the British Standards Institution responsible for standardisation in the business sector including Information and Communications Technologies (ICT).

Within the framework of BSI, DISC's mission is to help Enterprises achieve their operational effectiveness by accelerating standardisation in information systems and by promoting standards and making them easier to exploit.

5. COMMON AND SPECIAL WORK PROGRAMMES

In addition to managing the resources allocated within BSI for Common Work Programme (CWP) activities in the ICT sector, DISC is empowered to raise additional resources (funding and in kind) and allocate them to Special Programmes (SP) according to priorities agreed with the sponsors and within DISC's remit.

The CWP encompasses the ICT standardisation in international (ISO/IEC, ITU) and European (CEN/CENELEC, ETSI) committees as well as purely national work, where demand exists. The areas include advanced manufacturing, information and documentation, information systems and telecommunications.

Among others, within its Special Programme DISC has prepared guidance on the millennium issues, legal admissibility of electronic documents, and information security management. It also works with individual partners or groups to address specific business issues (eg the UDC Consortium, TickIT).

Annex**ADDITIONAL INFORMATION**

Standardisation [ISO/IEC Guide 2: 1996, definition 1.1]

Standardisation is the activity of establishing, with regard to actual or potential problems, provisions for common and repeated use, aimed at the achievement of the optimum degree of order in a given context.

[Note 1. In particular, the activity of the processes of formulating, issuing and implementing standards.

Note 2. Important benefits of standardisation are improvement of the suitability of products, processes for their intended purposes, prevention of barriers to trade and facilitation of technological co-operation.]

20 November 1997][Continued

Standard [ISO/IEC Guide 2: 1996, definition 3.2]

A standard is a document, established by consensus and approved by a recognised body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

[Note. Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.]

Consensus [ISO/IEC Guide 2: 1996, definition 1.7]

Consensus is general agreement, characterised by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments.

[Note. Consensus need not imply unanimity.]

The impact and use of ICT in the 1990s

Information and Communications Technologies (ICT) applications not only pervade most businesses today, but those businesses increasingly depend upon ICT for their growth and success.

Not only are the technologies in any case rapidly developing, but exploitation by those businesses of ICT facilities and their demands for “more; better; faster” also generate and impose increasing demands on the ICT suppliers or service providers to accelerate change.

A significant majority of ICT standardisation (perhaps 70 per cent?) is *de facto* but the major suppliers also support *de jure* standardisation for their own mutual benefit and where user and political pressures have an impact. For the most part, the facility that enables their participation and influence via BSI is of primary value, but the resultant *de jure* standards generally have low sales potential, because only a few organisations need to directly apply them. On the other hand, their application (alongside *de facto* standards) affects almost all ICT products or services and their application.

What BSI facilitates in consensus standardisation in the ICT area always has been, and remains today, high-profile, technically complex, costly, fast moving and non-profitable. The lack of sales potential here is no indicator of value of the product. Also, because of the rate of change in the sector, key international and European standardisation processes have become significantly more productive than their predecessors and their non-ICT counterparts in meeting customer requirements, and have been held as models for others to emulate.

Only a tiny part of the almost universal business-wide demands on the ICT communities supports ICT standards-making: mainly, it is the ICT manufacturers and direct users that underpin BSI activities in ICT. In only a very few areas (eg software quality [TickIT], information security [BS 7799], Millennium Bug [PD 2000]) do business-wide demands result in a significant contribution to the ICT sector in BSI, and then mainly through standards-related business rather than formal standards.

In direct response to stakeholder demand and sponsorship, DISC has a growing key function in the non-consensus standards-generating arenas, whether as honest-broker or partner, and is respected in the formal, open consensus arenas. The high status of BSI and DISC enables influence to be exerted and encourages would-be competitors to collaborate to generate widely-acceptable best practice or informative guidance material.

20 November 1997]

[Continued

Examination of Witnesses

MR ALAN SHIPMAN, Group 5 Group, Editor of the BSI Code of Practice, and MR ALAN STEVENS, BSI, called in and examined.

Chairman

183. Mr Shipman, Mr Stevens, may I thank you both for coming to give evidence this morning and thank you also for the written evidence which you submitted. Would you for the record perhaps introduce yourselves and then we can get on with our questions?

(*Mr Shipman*) My Lord Chairman, thank you, and thank you for the invitation. My name is Alan Shipman and I work as an independent consultant. I have been around 25 years in information management. I chair a number of BSI and industry committees in the area of information management, including an international meeting, an International Standards Organisation committee, on document imaging quality. That is where I am coming from, my Lord Chairman.

(*Mr Stevens*) My Lord Chairman, I am Alan Stevens. I have been employed by the British Standards Institution in the standards making area for some 24 years. I currently manage the department that is responsible for information and communications technologies' standards.

184. Thank you very much. Are there any opening remarks that you would like to address? If not, we will go straight to the questions.

(*Mr Shipman*) I am happy to go straight to questions, my Lord Chairman.

185. Perhaps I may invite you to share the questions as you would wish. May I start then by asking whether you could provide us with a very brief outline of the features of the British Standards Institution's code in so far as it relates to document authentication?

(*Mr Shipman*) My Lord Chairman, the code has been developed really in the period 1993 to 1996 where document imaging was in its infancy. It is very much a procedural document. It does not really talk about the technology; it talks about how people do things, and it talks about the need for documentation and the need for audit of such systems. In particular, where documents are needed to be used as evidence, and I will come back to what I call a document in a minute, it does talk about what procedures you should use for the authentication of those documents, particularly things like quality control—how do you know that you have a good quality image. I was listening to the previous witnesses, my Lord Chairman. I think that we may need to talk to them later; I think that we may have some advice for them. What do I call a document? I think that is important. A document is just a piece of information, the medium does not matter. Here we are talking about information and your committee title, my Lord Chairman is Digital Images, and that image can

contain anything: it can be a video, it can be a voice, it can be a document, it matters not to me.

186. Thank you, Mr Shipman. Mr Stevens, would you like to add anything?

(*Mr Stevens*) My Lord Chairman, no, I have nothing to add.

Baroness Hogg

187. What were the industrial demands that prompted BSI to develop the code on the legal admissibility of documents? Where did the problems arise and what sectors of industry felt the need for something to be done?

(*Mr Shipman*) My Lord Chairman, there were two quite distinct groups of people who in 1993 got interested in what ended up to be a code of practice but really they were having difficulties with the technology and saying, "Yes, this looks like a good idea for storing our documents but we have this problem of, are they legally admissible at the end of the day?". One group was the suppliers. They obviously wanted to sell their systems and they were getting resistance. One of the things that they were saying was: you can scan your documents in the system and you do not need to keep the original paper. But, of course, the users were then saying: well, what about when I need them in court, how do I deal with that? Therefore, the suppliers had a problem and they started some work with the Computer Supplies Federation working in that area. The users also could see the advantages of the technology and they wanted to do it, but they again had the same problem—what about the court, what about the industry regulators, would they accept it? So they started to do some work, quite independently actually, my Lord Chairman. There was an inaugural meeting at Cranford University in 1993 where 150 people got together to discuss this, and that formed the basis of some work that they did. I got involved—and I only got involved in 1995—from chairing one of the industry groups. I looked at these two different bits of work and thought, really they should be one, really that should be brought together and really our friends from the British Standards Institution ought to be the people that published it. That is how it developed, that is the idea behind it.

Chairman] Perhaps we may move on now.

Lord Flowers

188. Was it difficult to get people to agree on what was necessary?

(*Mr Shipman*) In all honesty, my Lord Chairman, there were no real problems with it. People wanted it, people wanted to do it. Perhaps one could say that the only problem that we had was the time that it took to do it. It was all done voluntarily. A lot of people put a lot of time into producing it. Yes, my Lord Chairman, there are always problems with doing these types of documents with the words themselves and writing words that people would understand.

⁴Footnote by witness: Our proposal for a code of practice enshrined in statute, whether or not coupled with a system of licensing, is to address our concerns about voluntary regulation. We believe that in most instances codes of practice developed by trade associations are voluntary in nature.

20 November 1997]

MR ALAN SHIPMAN AND MR ALAN STEVENS

[Continued]

Lord Flowers *contd.*]

189. In that case everybody has accepted it, I presume?

(*Mr Shipman*) My Lord Chairman, yes.

190. No exceptions?

(*Mr Shipman*) Not that I am aware of, no.

Chairman

191. And we are talking about the United Kingdom now. Nowadays, of course, many of the documents are produced by global international companies, not necessarily even subject to United Kingdom law. What perceptions have you there? Are there problems? Do we need a global code?

(*Mr Shipman*) Absolutely. There are a number of opportunities in those areas. We have looked at work being done in America and in Canada and in various European countries and fairly recently Australia. They have all done work in this area, but they have all looked at the technology, they have all said, "Do this, do this, do this"; they have not done it from a procedural point of view. They have looked at the work we have done and they have seen the benefits of that approach where the technology really is not the prime mover and they have accepted what we are doing, and those countries that are on the relevant ISO committee have taken our draft and that is now on the stocks as a potential publication. So, yes, they are very interested in what we are doing. In fact, only a couple of days ago I did some work for a utility looking at wayleave documentation and scanning that information on and keeping it electronically. They had a visitor from America who was very interested in what we were doing and saw the code of practice and immediately grabbed it and rushed off with it. He was very interested in it. He wanted to see it—"We have got nothing in the States like this", was his comment. I was not there at the time, so it was not just me who told him about it. I think therefore that we have something; I believe that for once the United Kingdom is leading the world in this area and, yes, you are right, it is an international issue. We have also had a number of discussions with the European Union and they have also got people working in this area and are very interested in what we are doing.

192. Mr Stevens, is there anything that you would like to add? I had the privilege of going to Chiswick last night on a visit to the British Standards Institution.

(*Mr Stevens*) Congratulations! My Lord Chairman, yes, may I simply add that although the code in question was developed in the British Standards Institution context a number of the organisations that were consulted and contributed were in fact multinational organisations and even those that are purely national do engage in international trade, so there is really already an international element of consultation.

Baroness Hogg

193. But to what extent—and I am very happy that we are leading the way—does this fall foul of different national legal systems? We can think of some that have not even moved to the written word:

some exchanges of contract in Switzerland have to be read out loud. They are a long way from digital information there. Can you tell us something about that, how will it be resolved, in what forum—the ISO? Where will it be resolved.

(*Mr Shipman*) Indeed, my Lord Chairman, and we actually side stepped that issue by simply saying, you obviously know which countries you are dealing with, you need to look at the local laws and you need to look at the local regulatory bodies and see what they require. We do not give legal advice on the code of practice, we simply say who you need to talk to, what you need to do. If you like, therefore, we side step the issue.

194. So you are not answering the issue, will this document be admissible in a court?

(*Mr Shipman*) We cannot say that, it is not something that we can do.

195. You explained that the driver for this work was the suppliers wanting to be able to tell people that their systems would produce documents in the form you decided could be used in court. It does not seem to me therefore that you have satisfied them.

(*Mr Shipman*) Absolutely, my Lord Chairman, and that is our big problem.

196. Right!

(*Mr Shipman*) That is our big problem, we cannot say. That is all that we can do, absolutely. All that we can do is to say, run your system in the best possible way, be as confident as you can that the information that you are keeping on your system is secure and that it has not been changed. That then gives you the best chance in court. It would be wonderful if it was the other way round and if the courts and regulatory bodies said to us: yes, okay, we will accept electronic documents as long as you comply with the code of practice. There are a number of regulatory bodies that are considering it. There are a number of companies that themselves have taken the decision: yes, if and when we comply with the code we will not keep our original documentation. This is because they have evaluated the risk of not keeping that old paper.

197. And they have taken the decision?

(*Mr Shipman*) They have individually taken the decision. It would be nice if it was the other way round.

Lord Ackner

198. If I may just follow that point up, my Lord Chairman, there are really two points. One is the admissibility of the documents. The other is the weight which is given to those documents once it is admitted.

(*Mr Shipman*) Yes.

199. And you are seeking, assuming it is going to be admitted, to be able to say to your client: you will get the maximum weight attached to your document because you have followed what we tell you as experts is best practice?

(*Mr Shipman*) Yes, absolutely right. In fact, just to go a little further than that, with all the clever things

20 November 1997]

MR ALAN SHIPMAN AND MR ALAN STEVENS

[Continued]

Lord Ackner *contd.*]

that you can do with paper these days, is an electronic system secure or safer than a paper system?

(*Mr Stevens*) My Lord Chairman, may I perhaps add two small points. The code of practice, although it has the label legal admissibility in fact defines the best way of storing documents and carrying out audit checks so that it can be demonstrated once you have only the copy in whatever form the copy exists it is as faithful a reproduction of the original as can be verified. That is point one. Secondly, my Lord Chairman, this code is one of a related set of codes dealing with the wider subject of information management in general and information security techniques. The previous presentation could very easily relate to the set of documents on information management because, as Mr Shipman said, information stored on closed circuit television is just information and the management of that information is what we are really concerned about, to do it the best possible way by the mutual agreement of all the parties concerned with handling it.

Chairman

200. So in effect you are recommending, are you, something like what we were talking about earlier this morning, that that code of practice could be strengthened by following a BSI type code?

(*Mr Stevens*) I would not be so bold as to say that, my Lord Chairman. It certainly sounds as though there is a relationship that needs to be looked at.

Lord Brain

201. So in effect you could just as easily apply this code of practice to the old fashioned way of microfilming all documents as you could to putting it on computer?

(*Mr Shipman*) Indeed, my Lord Chairman. You could actually apply it to a paper system even. But, yes, oh yes, microfilm was the very first worm medium.

Lord Kirkwood

202. The code has been completed, the objective has been met. That is what I take it you actually said a few minutes ago, but I was then slightly confused by your saying it was not fully acceptable, this evidence, but it was the best that could be done. However, as far as you are concerned the objective has been met and there is no further work, no further research, that could be done to enhance the quality of the evidence?

(*Mr Shipman*) No, my Lord Chairman, I do not agree with that.

203. I am not sure what you do not agree with—the final statement?

(*Mr Shipman*) The problem that we have again is that technology is moving. The codes were developed and published in 1996, as I say. People are using document imaging systems, for example, in work flow systems and wish to retain evidence of the work flow system to back up that documentary evidence, so there is work going on in that area.

204. But what you are suggesting is technology free, is it not?

(*Mr Shipman*) Sure.

205. You said it can apply to anything?

(*Mr Shipman*) Oh, yes.

206. So advances in technology do not influence the procedures that you are talking about?

(*Mr Shipman*) The code also very much talked about worm medium because that was the only optical medium, the only high volume storage medium, that was around at the time. We all know with much bigger magnetic stores and with re-writable optical media now people are wanting to store on that type of media. Okay, there is an area where technology has moved past the code.

207. It has?

(*Mr Shipman*) It has in that instance, and we need to put further recommendations into the code in terms of how to deal with that. So, yes, we did specifically talk in the code about a particular type of storage media in terms of worm but now it has moved on.

208. But you could not describe your system in which it was free from the development of technology by saying it did not encompass anything likely to improve the technology?

(*Mr Shipman*) Oh, yes.

209. You could?

(*Mr Shipman*) Yes.

210. And you will do that?

(*Mr Shipman*) Yes. There is also authentication and this is in question number five, I think, so perhaps I will leave it.

Lord Brain] I was just about to ask that question.

Chairman] We will invite Lord Brain to lead you on question number five.

Lord Brain

211. I think that we have got there really, my Lord Chairman. It is really the use of technology like, for example, watermarking to provide what you have already described, the audit trail, and no doubt you heard my question to the previous team: how does one deal with this on worm devices of the modern era? It was easy on microfilm.

(*Mr Shipman*) That is right, and there is nothing in the code about these techniques. They were not really available when we were producing the code. There are in fact new codes being developed in this area. The current code is staying as it is, as a storage code, but in terms of authenticity of documents, which is what we are talking about here, new codes are being developed again in conjunction with people like BSI in this area. There are lots of interesting discussions going on. Yes, you can digitally sign, you can watermark a document today, and it is reasonably secure, but I am sure that in ten years' time you will have enough computing power in your wristwatch to break that code, so where do we go, how do we deal with all of that? That is currently being worked on—in a different area in terms of authenticating documents before they become under the control of the storage code, how do you authenticate something

20 November 1997]

MR ALAN SHIPMAN AND MR ALAN STEVENS

[Continued]

Lord Brain *contd.*]

before it is stored away, and that is where that work is coming from.

212. So that what you are saying in effect, Mr Shipman, if I may just summarise, is that you have got the storage capability?

(Mr Shipman) Yes.

213. There is going to be another BSI standard perhaps on authentication of what is to be stored which could be applied to anything that came from a video camera which is a source of digital information, there will be a code to identify them?

(Mr Shipman) This is the recommendation from the company that I work for to BSI, and we are currently looking at the words.

Chairman

214. But there is a technology there which you feel will meet this requirement?

(Mr Shipman) Yes, my Lord Chairman, today there is.

Chairman] If there are no further points on that, we will go to question number six, Lord Ackner.

Lord Ackner

215. I think that you made it quite clear that this is a voluntary code?

(Mr Shipman) Yes.

216. And there is no need in your view to require that it is complied with as a matter of law. That is the position, is it?

(Mr Shipman) That is certainly the position, my Lord Chairman, yes. It would be nice, again on my wish list, if the law in some particular area of record keeping, a regulatory body, said that: yes, if you store your documents under the control of the code we will accept them—then, yes, that may change the question round. It may not then be voluntary to those people if they wish to do it that way, if they wish to keep their documents electronically and their regulator says, we will accept them, is it still voluntary or ought there to be some scheme to check.

217. He would be quite happy with the court saying, this is the best practice, we therefore give the greatest weight we can, the best practice having been found, and you cannot improve on that position?

(Mr Shipman) That is correct, my Lord Chairman.

218. I have not quite followed what is your experience in regard to the action taken by other countries whom you have consulted.

(Mr Shipman) I cannot think of any specific cases, my Lord Chairman. Electronic documents are used in courts very frequently, they are used all the time, and they are accepted. To date I have not heard of any case where an electronic document has been thrown out of court because it was an electronic document. There are many cases of there being questions, but being able to be understood and then explained and then to be accepted. I am aware, I do not know whether an experiment or a real case in South Australia where the Government does everything electronically. All the Bills are published electronically, all the records of meetings are

published on the web, etcetera. That is obviously of great interest to us. I suspect that they also produce paper copy for their records, but, yes, more and more people are getting into the area.

Chairman] Then question number seven, do you want to ask any more, Lord Ackner?

Lord Ackner] No, I do not think so, my Lord Chairman.

Chairman] Are there any other points that Mr Shipman or Mr Stevens would like to make?

Lord Brain

219. If I may ask a slightly related question, my Lord Chairman, we were talking about digital images. Digital images are often considered to be photographs. Do you feel that enough detail and care can be scanned into a system to be certain that it will not be modified after it has been scanned in if it is required to be used as evidence? I was thinking of medical photographs and things like that which may be held, and probably would be held, I suppose many years after there had been an accident. If there was some consequential problem and the photographs had been mislaid but they had been recorded electronically, do you feel that you could produce a satisfactory assurance that those photographs had not been tampered with to produce the result in evidence that is then required at a much later stage?

(Mr Shipman) Okay, may I answer stage two, because there is the producing of the electronic image first and then there is a storing and being able to show that that has been changed as a second part to that. The second part I can do first because that is easy, and that is how the code works, on making sure you have got back what you put in. Then in regard to the first part of the question, can you actually achieve a good enough image from the original, be it a photograph or whatever it is. You are always going to lose something. You are going to lose the actual paper that it was written on from a forensic point of view, "Was that piece of paper written in the 1930s or the 1940s?" You lose that sort of evidence. You lose the type of ink from the signature, so you have got to evaluate each particular type of document, each particular application, and say: on my imaging system am I going to retain enough evidence for when I am going to need to produce it in fact in the nuclear industry in 150 years' time, because that is what their retention periods are, and you have got to look at each individual case to decide whether you can in fact keep enough. Then again, going back to that four letter word, risk, what risk am I taking. There are substantial cost benefits to be achieved by keeping everything electronic and not keeping the paper. I heard an estimate yesterday in a particular case of a 70 per cent reduction in the cost of storing information by doing it electronically compared with paper, so people very much want to do that, but they are going to be taking a risk because they are going potentially to be losing something. Does it matter? If it is for a ten pound invoice, no, it does not matter, but if it is for a contract to build a bridge on which you have got two original signatures, perhaps you do keep that piece of paper.

20 November 1997]

MR ALAN SHIPMAN AND MR ALAN STEVENS

[Continued

Chairman

220. Thank you very much. May I thank you and ask, are there any other points that we have not covered that you felt you would have liked us to ask you about?

(*Mr Shipman*) My Lord Chairman, I think in that last area I brought out all that I wanted to.

(*Mr Stevens*) If I may add something, my Lord Chairman, it has sort of been hinted earlier that none of the standards, none of the codes of practice, will have any value unless they are actually used. The ultimate test of this one is that admissibility can only be in the courts. There has to be a legal challenge and it has to be either accepted or rejected, and then we will know the true value of what is written. Secondly, and in some respects it relates to the previous presentation, there is a very great deal of customer clout that is available in using codes of practice and in insisting on having suppliers that will meet the requirements in those codes. It does not need legislation; it needs the customers to get together to

exercise the buying power that they have. Finally, my Lord Chairman, the British Standards Institution is also working at the moment in collaboration with the Public Record Office on a project called Eros, which you may well know about. It is an electronic record from office systems. I am well aware that the Public Record Office secretariat of the BSI committee doing that work is trying very hard to get international collaboration, so whilst we are doing work within the British Standards Institution participation is coming from America and other parts of Europe as well.

221. Thank you for raising that last interesting point, Mr Stevens. May I thank you both, Mr Shipman and Mr Stevens, very much indeed for coming to see us and being so helpful with your replies to our questions and, indeed, for the written submission that you have supplied us with. Thank you very much.

(*Mr Shipman*) Thank you, my Lord Chairman.

(*Mr Stevens*) My Lord Chairman, thank you.

THURSDAY 27 NOVEMBER 1997

Present:

Ackner, L.
Craig of Radley, L.
(Chairman)
Flowers, L.
Hogg, B.

Howie of Troon, L.
Kirkwood, L.
Leicester, Bp.
Nathan, L.
Phillips of Ellesmere, L.

Memorandum by the Deputy Data Protection Registrar**CCTV SYSTEMS AND THE DATA PROTECTION ACT**

To be covered by the Data Protection Act 1984, the data captured on CCTV systems must be personal data processed automatically by reference to the data subject, within the definition contained in the Data Protection Act. To answer the question of whether a given system fits that definition a number of specific questions must be addressed.

1. IS IT DATA?

Data is defined as:

"information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose"

Clearing the recording of images on the medium of video tape is little different to the magnetic media used in conventional computing, and it is a form which can be processed automatically.

2. IS IT PERSONAL DATA?

Personal data is described as:

"data consisting of information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user), including any expression of opinion about the individual but not any indication of the intentions of the data user in respect of that individual".

The simple recording of video images about unknown individuals may not meet the terms of this definition as it does not relate to living individuals who can be identified from that and other information in the possession of the data user. However, there may well be circumstances where a video image is of a known individual, who can be identified from that or from that and other information in the possession of the data user. This may well be the case where the video image is used in a crime investigation or for evidential purposes purporting to show a known individual committing a particular offence. This would also be the case where the CCTV system is installed by an employer in his or her premises and will capture images of that employer's employees.

3. IS THE DATA PROCESSED AUTOMATICALLY BY REFERENCE TO THE DATA SUBJECT?

Processing is defined as:

"amending augmenting, deleting or rearranging the data or extracting the information constituting the data and, in the case of personal data, means performing any of those operations by reference to the data subject".

Certainly information may be extracted about an individual by viewing his activities recorded on tape. However, it is not just the processing operations themselves that must be automated. The way in which the equipment performs one or more of these operations "by reference to the data subject" must also be automated. Thus equipment which can respond to instructions requiring it to locate and process information about an individual is capable of processing personal data. The instructions need not necessarily involve the equipment being given a name, account number or other identifier. The equipment could, for example, be given a time or frame reference to a location on the tape at which it is known information about an individual is recorded. If the equipment then moves automatically to this location it will be capable of processing personal data within the terms of the Data Protection Act. If the equipment is not capable of automatically

27 November 1997]

[Continued

locating particular information stored on the video tape, it is unlikely to perform operations that are regulated by the Act.

If the operation is covered by the Data Protection Act then the requirements are that a person or organisation registers the type of personal data that is held, the purpose for which it is held, from whom it was obtained and to whom it will be disclosed. The data must also be obtained and processed in accordance with the eight Principles of the Act. A use or disclosure of the data that goes beyond the register entry or that is not in accordance with the Principles will be a breach of the Data Protection Act and could amount to a criminal offence.

The First Principle of the Act requires that:

"The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully".

The courts have held that, for data to be obtained fairly, individuals must be informed in advance of any non-obvious uses of disclosures that will subsequently be made with their data. I would suggest that the logical application of this rule to the operation of CCTV systems is that people must be notified that there are cameras in operation.

There are more complex questions about what form this notification should take, whether it should inform people of who is operating the camera and for what purpose. However, for the time being, until we have produced comprehensive guidance on this area, it is suggested that the minimum requirement would be to place readily visible notices at locations throughout the site informing people that there are cameras in operation.

The other Principles of the Act require that data is:

- Held only for the purposes specified in a data users register entry.
- Used only for the purposes and disclosed only to the people as described in the register entry.
- Adequate, relevant and not excessive in relation to the purpose for which it is held.
- Accurate and, where necessary, kept up to date.
- Held for no longer than is necessary.
- Held securely to prevent unauthorised or accidental access to, alteration, disclosure, loss or destruction.

It is also a fundamental aspect of the Act, that individuals must be allowed access to information held about them (unless certain limited exemptions apply).

You will appreciate that it is difficult to advise on specific uses of CCTV systems without full details of the system and its operating procedures. The application of the Data Protection Act to CCTV systems raises complex questions which may not have been addressed previously (for example, what is sufficient notification? How should subject access be facilitated?) These grey areas are yet to be resolved, this office will be producing guidance on these matters. In the meantime the Registrar would accept that it would be extremely difficult and inappropriate to take formal legal action against an organisation that had approached us for advice. However, this would not detract from the Registrar's duty to investigate complaints and promote compliance with the Act. In this context, if any breach of the Act did come to light the Registrar would seek to ensure compliance by way of negotiation and discussion.

The Office of the Data Protection Registrar has produced a booklet called "*The Guidelines*" which explains these concepts in greater detail and covers the application of the Act as a whole and should address any general questions you might have.

Memorandum of the Data Protection Registrar

INTRODUCTION

1. The Data Protection Registrar is grateful for the opportunity to submit evidence in response to the Sub-Committee's request. In principle, the Registrar shares the concern expressed in the call for evidence that because of ease of copying and manipulation of digital images, there is a risk of improper use and the evidential value of digital documents can be prejudiced by uncertainty about originality and the accuracy of copies. The Office has not had experience of using digital images in evidence, but the Registrar would like to take the opportunity of commenting from a policy rather than a technical point of view on some of the issues raised. The Registrar particularly wishes to comment on CCTV surveillance systems of which the Office has had some experience.

27 November 1997]

[Continued]

GENERAL REMARKS

2. The primary rôle of the Registrar is to enforce the Data Protection Act 1984. That Act broadly requires those who keep information on computer about living individuals to register and then to comply with a code of good information-handling practice set out in eight Data Protection Principles (Annex A). The 1984 Act is derived from the 1981 Council of Europe Data Protection Convention¹ and ultimately from Article 8 of the European Convention on Human Rights² which guarantees to individuals the right to private life. Data protection as protection of the privacy of individuals is confirmed by the 1995 EU Data Protection Directive 95/46/EC, Article (1) of which provides that:

“Member States shall protect the fundamental rights and freedoms of naturalised persons, and in particular their right to privacy with respect to the processing of personal data.”

The Registrar therefore approaches issues raised by digital images from the standpoint of seeking to protect the informational privacy of individuals.

3. As the Registrar understands the law in England, the courts will, when appropriate, treat computer records in an equivalent way to written documents. So information held on computer has been held to be equivalent to a document for the purposes of discovery in civil proceedings, *Derby & Co Ltd and Others v Weldon and Others* (No 9) [1991] 2 All ER 901. Destruction of a computer record may be contempt of court, *Alliance and Leicester Building Society v Gahahremani*, Chancery Division reported in *New Law Journal* March 1992. There is no doubt that a computer record can be the subject of a warrant application and seizure under a warrant, *R v City of London Magistrates' Court and another ex parte Green* [1997] 3 All ER 551.

4. This implicit policy of the courts is to be encouraged. The Registrar is strongly of the view that both electronic commerce and electronic service delivery by government can bring benefits to individuals in access to services whilst benefitting purchasers and taxpayers by reducing cost. It is, however, important to establish an adequate legal and technical infrastructure to encourage those developments and give confidence to those using the new information technologies.

THE SUB-COMMITTEE'S QUESTIONS

5. Question 1—The Registrar is aware not only from the literature but also from visits to television broadcasters that digital technologies are extensively used for the transmission and storage of images of individuals and that those images can be readily manipulated. Some manipulation might be the benign equivalent of the modifications often made to photographs for artistic or presentational reasons. There is scope for more extensive manipulation which can lead to misrepresentation of the original image. It would be helpful to be able to identify readily which variation of an image was the original in any case of dispute. It should be remembered that the original might have been an analogue image subsequently digitised with possible loss or modification of information.

6. Questions 2 and 3—There are risks to the use of digital images as evidence, against which special precautions can be deployed. If a digital image is to be used as evidence, then currently special procedures are required to authenticate the image. The evidential rules relating to the use as evidence of any computer record—including images—depend on separate evidence of system integrity. This can be compared to provisions governing the use of conventional photographs, where evidence has to be given connecting the print to the negative and confirming that the negative is untouched. Whilst the Registrar accepts that greater risks might attach to an assumption of authenticity and integrity of an image than of a text document, the Registrar's view is that these evidential problems arise in the case of all digital documents such as those created in Electronic Document Interchange (EDI) transactions.

7. The Registrar suggests that encryption techniques may be a means of authenticating an original digit image and of identifying whether further copies are in an altered state. Cryptographic methods can be used not only for confidentiality of storage and transmission, but also as a form of electronic signature. If such an approach were adopted to “signing” images, consideration should be given to whether the absence of a digital signature would destroy the evidential value of the image, merely weaken it, or whether new systems of authentication could co-exist with existing ones. A view would need to be taken of how to deal with currently existing documents and images and what incentive would encourage the adoption of stronger systems. In the absence of standard systems and protocols, the interim step might be to give statutory encouragement to the adoption of any such technique as will tend to convince a court of the authenticity and reliability of the image. If the result were that evidence of different strengths of reliability became available, thought would also need to be given as to whether in some types of case—eg criminal cases—only the most reliable digital evidence should be admitted.

¹ Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series No 108, Strasbourg 1981.

² Council of Europe Convention for the protection of human rights and fundamental freedoms European Treaty Series No 5.

*27 November 1997]**[Continued]*

8. The Registrar would draw the Sub-Committee's attention to the recently published OECD guidelines on cryptography³ which encourage the free market development of strong cryptographic methods to facilitate the development of international electronic commerce. Those guidelines clearly recognise the distinction between the use of cryptography for confidentiality and for authentication. If cryptographic methods are to be used then some assurance needs to be given of the reliability and strength of those methods. It is also most important to guarantee the secrecy and security of encryptions keys used for authentication purposes. Trusted Third Parties (TTPs) might have a rôle in giving that general assurance; and in order to guarantee the reliability of TTPs licensing should be considered in the interests of the consumer, commercial parties and the reliability of the legal process.

9. The Registrar has seen proposals for "watermark" systems which have been developed principally for copyright control purposes. If the reliability of these systems can be demonstrated, then they have a valuable rôle to play in demonstrating authenticity. Perhaps some variant of the technology could be used to indicate whether a copy had been altered because, as the Registrar understands it, the point of "watermark" is to retain the code through whatever transformation the image might pass.

10. The Registrar is unable to suggest a preferred technology. Experience needs to be gained of the techniques available, their value to users and to the courts. Any new law at this stage should give incentives to develop valuable techniques without prescribing a specific solution.

11. Question 4—The Registrar recognises that image enhancement can be a valuable technique, but has anxieties about the use of modified or enhanced images of individuals. The issue has already arisen in the use of CCTV images in high-profile criminal cases. The techniques used to modify or enhance need to be demonstrably proper. It is not always apparent that the procedures used to enhance images produce a proper likeness of an individual. From the Registrar's point of view, where digital techniques are used, enhancement raises questions about compliance with the Data Protection Principles. Can the technique be said to be fair processing (First Principle)? Can the result be said to be accurate (Fifth Principle)? Is the resulting image adequate or relevant for its purpose (Fourth Principle)? If enhanced images fail these tests, then the data user is in breach of the Data Protection Act 1984 and that would question the appropriateness of such images as evidence. Perhaps the tests set out in these Data Protection Principles might form part of the controls permitting the use of modified or enhanced images.

12. Question 5—The Registrar does not feel able to respond to this question.

13. Question 6—Whether surveillance cameras, in conjunction with image tracking software or not, threaten civil liberties, will depend on how they are used. Thus systems that are used to monitor public spaces may have different effects on the individual from those which are used to monitor private spaces. For example surveillance systems that are installed in a workplace to monitor staff activity may have different implications from cameras mounted in a city centre which survey crowds or large numbers of unidentifiable individuals. It is not so much the existence of technology that poses a threat to the civil liberties of the individual but the use that is made of technology and the setting in which surveillance takes place.

14. An illustration of this would be the police use of tracking equipment to view faces in a football ground in order to locate known football offenders. In such cases, the use of surveillance equipment can be useful to the police authorities where they know or have reasonable grounds for believing that an individual or group of individuals has been involved in criminal activity. Short term covert surveillance used to target specific individuals in a specific area or carrying out a specific activity may be an acceptable use where criminal activity is suspected. However, the use of such technologies to track individuals where there are less substantial grounds for suspicion or where the activity involved is not criminal, may well have a detrimental effect on civil liberties. Moreover, constant indiscriminate covert surveillance may constitute a breach of civil liberties where there is no real target or objective to or grounds for the activity—for example, the recording of individuals' movements by capturing the registration details of vehicles travelling along motorways.

15. It is therefore difficult to say that these technologies threaten civil liberties in all circumstances. However, the potential exists, and relevant safeguards are appropriate to ensure continued public confidence in activities such as town centre surveillance. At present, many organisers of such schemes are preparing voluntary codes of practice in relation to their use of such technologies. To assist in this, the Local Government Information Unit has produced a model code of practice for use of town centre surveillance schemes much of it based on the standards set down in the Data Protection Principles.

16. Question 7—To a limited extent there are already statutory controls on the use of surveillance cameras and the release of information from them. Such systems may need to be registered with the Data Protection Registrar if they record and process personal data by reference to the data subject. Thus the limited number of surveillance schemes where the image retrieval system can be programmed to locate specific images on the recording medium, will need to be registered. As a result of registration, such systems will also need to comply with the Data Protection Principles. A fundamental aspect of data protection is that information should be collected for specified and legitimate purposes and used and disclosed only in ways compatible with those

³ OECD Cryptography Policy Guidelines—Recommendation of the Council concerning guidelines for cryptography policy—27 March 1997.

*27 November 1997]**[Continued]*

purposes. The Registrar would welcome the clear application of that principle to surveillance systems to the extent that it does not already apply.

17. Between the requirements of registration and the need to comply with the Data Protection Principles, there is already a basic level of control over the use of not only the systems but also the information provided by the systems. For example in deciding whether the information from a system had been obtained fairly, the Registrar would consider such matters as the location of the camera, and whether appropriate notice had been given of its existence. Many system users make use of notices to announce the existence of the system, not simply because that complies with the 1984 Act, but also for their deterrent effect. In addition, the other Data Protection Principles set out standards which may have to be complied with. These include the requirement for images to be relevant and not excessive (Fourth Principle), not retained for longer than necessary (Sixth Principle) and made available to individuals on request (Seventh Principle). The Principles' requirements in relation to the fairness of the processing, accuracy and the adequacy of the information recorded may be particularly relevant when considering the use of enhancement or compression techniques as mentioned above in response to Question 4.

18. Although the limitations of most current surveillance systems mean that they fall outside the scope of the 1984 Act, the increasing sophistication of equipment involving the capture of digital images and computer aided retrieval will mean that increasing numbers of such operations fall within its scope. Recitals 14 and 16 of Directive 95/46/EC make clear that the processing of sound and image data are in principle within the scope of data protection law. Domestic data protection legislation will have to take account of this by 24 October 1998 and the Government has announced the intention to strengthen data protection legislation with a Bill being introduced this autumn. The Registrar has previously called on the government⁴ to ensure that any opportunities afforded by the implementation of the Directive are seized in relation to CCTV surveillance in order to make regulation more consistent.

19. Question 8 — Conventional documents tend to carry certain inherent marks of authenticity and usage. A problem of all computer records not just digital images, is that the convention clues which accompany a written document are missing. Further, the techniques for processing images are so sophisticated that considerable technical expertise is required for a full understanding of them.

20. Perhaps what is required is sufficient familiarity with digital information technologies that their capability and risks are well understood by everyone. That is a question of long-term education for living in the information society. For those educated in an earlier world, some catching-up training would be valuable. The approach should be that of teaching someone to drive rather than to build the car. Users must know the strengths and weaknesses of the system and when it is being pressed too far.

21. Question 9 — The Registrar takes the view that where media organisations use fully automated systems, their collection and processing of personal information (including images) are covered by the Data Protection Act 1984. Directive 95/46/EC takes a similar position and provides in Article 9 that:

Processing of personal data and freedom of expression.

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and VI [the substantive data protection provisions] for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

The Registrar has sought to encourage a debate about how to strike the balance between the two fundamental freedoms of the right to private life and the right to freedom of expression.

22. A modified image might be defamatory and perhaps there might be other legal constraints to be satisfied. Proper artistic or presentational reasons for manipulation might exist. But, as drama-documentaries indicate, the creation of a fictional work based on real-life incidents can lead to confusion between truth and fiction. It is difficult to set up controls based on the motive for the modification. It would also, be preferable to avoid proposals which seemed to raise the issue of prior restraint of publication. If a modified image can still pass the tests set out in the Data Protection Principles, and is otherwise lawful, there seems to the Registrar no reason to restrain publication.

FURTHER ISSUE

23. The Registrar wishes to draw the attention of the Sub-Committee to a general evidential problem relating to the seizure of digital information. The issue arises whether data are seized in criminal proceedings under a warrant or in civil proceedings.

24. In order to demonstrate the authenticity and integrity of data seized, a law enforcement agency or a party to civil proceedings will prefer to download a whole database. This is likely to involve seizing material outside the scope of the warrant or order. The courts in at least one case have taken a restrictive view of what

⁴ Letter to the Home Office of 11 December 1995.

27 November 1997]

[Continued

should properly be seized (*Derby v Weldon* referred to in para 3 above). Some method needs to be developed to assure the courts of the integrity of what has been seized whilst protecting the rights of those subjected to such compulsory procedures. The Registrar recognises the problem, but has not identified a solution.

CONCLUSION

25. The Registrar is concerned to see developed secure and fair means of processing images digitally. There are risks in the uses of these technologies—especially where digital images are used as evidence—but the development of data protection law and the application of techniques such as strong cryptography should help to protect individuals.

F G B Aldhouse
Deputy Registrar

8 September 1997

Annex A

THE DATA PROTECTION PRINCIPLES

1. The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.
2. Personal data shall be held only for one or more specified and lawful purposes.
3. Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.
4. Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purpose or those purposes.
5. Personal data shall be accurate and, where necessary, kept up to date.
6. Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
7. An individual shall be entitled:
 - (a) at reasonable intervals and without undue delay or expense:
 - (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and
 - (ii) to access to any such data held by a data user; and
 - (b) where appropriate, to have such data corrected or erased.

Personal data held by data users or in respect of which services are provided by persons carrying on computer bureaux.

8. Appropriate security measures shall be taken against unauthorised access to or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

Data Protection and the Media—Article 9 EU Data Protection Directive

1. INTRODUCTION

This paper sets out to explain the way in which the Data Protection Act 1984 applies to the journalistic and related activities of the press and broadcast media. In the light of that explanation the paper goes on to discuss the implications of Article 9 of the recently approved EU Data Protection Directive⁵ (the Directive). The paper does not attempt to deal with the conventional processing of personal data by media organisations—such as mailing lists and personnel records—which is generally accepted as falling within the 1994 Act.

⁵ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities L281, Vol 38, 23 November 1995, ISSN 0378-6978.

27 November 1997]

[Continued

2. DATA PROTECTION ACT 1984

2.1 There is no exemption for the press, other media or journalists from the Data Protection Act 1984. Consequently, if a newspaper publisher or broadcaster holds personal data within the meaning of the 1984 Act, he must register with the Registrar and comply with the code of information-handling practice set out in the eight Data Protection Principles.

2.2 Old-fashioned newspaper production raised no issues within the scope of the 1984 Act. Commonly now, newspapers are produced with the aid of integrated computerised systems taking text from its origin with a journalist, through editing and production, to archiving of published newspapers. Those systems may typically be searched in numerous ways to obtain information about an individual. Indeed, we have now moved into the era of the electronic publication and distribution of newspapers. The technical questions to be answered are whether there exists "personal data", if so, whether it is "processed" and whether the processing is by reference to the data subject; and whether there is a "data user" for the data. Those key definitions are to be found in S.1 of the 1984 Act. The Registrar has developed and published guidance on these terms and their definitions and some assistance can be drawn from the few decided cases. That guidance is principally to be found in the Guidelines, the third edition of which was published by the Registrar in November 1994. In the Registrar's view and in the light of the statutory definitions, these modern production and publication systems are clearly within the scope of the 1984 Act and that is accepted by those newspaper proprietors who have registered appropriately under the 1984 Act.

2.3 Much the same can be said for broadcasting. Sophisticated editing equipment allows the ready manipulation of sound, image and text. All this can be done by reference to a particular individual. The 1984 Act refers to "information recorded in a form in which it can be processed . . ." These are the central elements of the definition of "personal data" in S.1 of the 1984 Act. "Information" can as well be conveyed by sound and image, as by text, and the 1984 Act control of personal data therefore applies to the journalistic and artistic activities of broadcasters. For ease, this paper often refers only to newspapers, but should be taken to refer equally to broadcasters unless a distinction is clearly drawn.

2.4 The Registrar has given some thought as to how this technological change might affect the legal duties of newspapers. The first data protection principle requires that information to be contained in data be obtained fairly and lawfully. That principle also requires data to be processed fairly and lawfully. The fifth principle requires data to be accurate and, where necessary, up-to-date. Subject access must be granted in accordance with the seventh principle and S.21 of the 1984 Act. The data must be adequate, relevant and not excessive for the purpose for which they are held (fourth principle). The data must be kept for no longer than necessary (sixth principle). There must be appropriate security (eighth principle). Data must be held for specified purposes (declared by registration) and not used or disclosed in a manner incompatible with those purposes (second and third principles). These eight principles must be respected by newspapers in relation to their publishing systems. They are set out in Annex 1 to this paper together with the statutory interpretation provisions.

2.5 There have been decisions of the Data Protection Tribunal which assist the interpretation of these principles—particularly in regard to fairness. In a decision on appeals brought by CCN Systems Limited⁶ and another, the Tribunal said:

"It is quite clear, from the Act as a whole and in particular from the data protection principles set out in Schedule 1, that the purpose of the Act is to protect the rights of an individual about whom data is obtained, stored, processed or supplied, rather than those of the data user.

In our view, in deciding whether the processing we have described is fair we must give the first and paramount consideration to the interests of the . . . data subject . . ."

The Tribunal in a subsequent decision on an appeal by Infolink Limited⁷ explained their use of the word "paramount" thus:

"We do not think 'paramount' bears the meaning that it is the only consideration, but rather the most important single consideration. In other words, we are to weigh the various considerations, and do so, but are entitled to give more weight to the interests of the individual . . ."

2.6 Fair processing issues might arise, but in a journalistic context one first thinks of questions of the fair obtaining of information. The 1984 Act tells us "regard shall be had to the method by which it (information) was obtained, including whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed". The implication of that provision is that information obtained by a journalist by a deception might well have been unfairly obtained and its use for publication could be restrained by the Registrar by enforcement proceedings.

2.7 Although the 1984 Act makes no special arrangements for the press or other media, and grants no specific exemption from registration, from compliance with the Principles, or from the duty to give subject access, the Act does exclude from its scope any computer processing operation performed only for the

⁶ CCN Systems Limited v The Data Protection Registrar (February 1991) paras 51 and 52.

⁷ Infolink Limited v The Data Protection Registrar (June 1991) para 65.

*27 November 1997]**[Continued]*

purpose of preparing the text of documents. It is possible that newspaper proprietors might be able to rely on this exclusion in certain cases where computerized systems are used purely for the production and publication of a newspaper. No electronic archives would have to exist if this provision were to be relied upon.

2.8 Although no relevant complaint has yet been made to the Registrar by a member of the public, she is aware of a potential difficulty in securing the right of subject access and related rights. Journalists keep notebooks which are treated by media proprietors as controlled by the journalists themselves. If those notebooks are in automated form the newspaper proprietor or broadcaster may have considerable practical difficulty in ensuring the right of access to a journalist's material. Where true control rests with journalists, it is they who should register under the 1984 Act and comply with the duties imposed on data users.

2.9 Concern has been expressed about the accuracy of information in the press. There are duties under the 1984 Act to ensure that data are accurate, and where necessary, kept up to date. It does not seem right to suggest that archive copies of published journals or broadcast programs should be subsequently amended in the light of changing events. That could be seen as an attempt to rewrite history. If, however, the system is providing an information database—even if drawn from published material of the particular publisher or broadcaster—different considerations apply and it might well be right to insist more rigorously that data be accurate and kept up to date. But in such a case, the accuracy principle could be recognized by a note of correction cross-referenced to the original material.

2.10 As mentioned above, the 1984 Act gives no special protection to journalists or the media. There is, in S 28, a limited exemption from the duty of subject access for any data user who holds personal data for the prevention or detection of crime or the apprehension or prosecution of an offender, if to give the data to a data subject in any particular case would prejudice those purposes. Journalists have expressed concern about giving data to those they are investigating. The policy of the legislation is not to give a specially privileged status to the police or other legitimate investigative bodies apart from the limited subject access exemption mentioned above. The Registrar would be reluctant to see an exemption given to journalists which gave them a status withheld as a matter of policy from the police and similar bodies. On the other hand she recognizes the significant role of the media and investigative journalism in our society.

2.11 For completeness, all eight data protection principles were mentioned earlier. Some of those principles will give rise to practical decisions of some difficulty: given the broad nature of journalistic activity, how is it possible to judge the adequacy, relevance and non-excessiveness of data for that purpose or to determine that it is no longer necessary to hold data? Nevertheless it seems that the principles raising the most important issues of practice and principle for journalists are those which require the fair and lawful obtaining and processing of data, the accuracy of data and the granting of subject access.

2.12 The Registrar can foresee circumstances in which a member of the public would ask her to investigate the publication of a newspaper story containing particularly sensitive information. Issues of fair obtaining and processing and of the accuracy and relevance of the information would undoubtedly arise in such a case. Personal data may be obtained not only from conventional interviews but might also be obtained from many automated sources by journalists, and compared as part of a piece of investigative journalism. In other contexts—for example, the comparison of tax and social security records as undertaken in some countries, or the compilation of direct marketing lifestyle profiles—considerable anxiety has been expressed about the cross-matching of automated files. Although the Registrar doubts whether journalists are currently matching information by the technical interlinking of files and running one against another, the technology is readily available, and the Registrar would certainly have concerns about data-matching for journalistic purposes.

3. A SCENARIO

3.1 The Registrar has considered how she might regard information to be found either in published newspaper articles or otherwise, held in a modern publishing system. It might be that information—whether or not of an especially discreditable nature—could be shown to be inaccurate. In such a case, the Registrar might have the power to secure by enforcement notice the correction or erasure of that inaccurate information. Moreover, under S.22 of the 1984 Act if the individual had suffered damage by reason of the inaccuracy of the data—as might be the case with particularly discreditable allegations—he could recover compensation for damage or distress attributable to the inaccuracy, subject to certain defences available to a data user.

3.2 The Registrar has also considered what her position might be if the data were found to have been obtained by some means such as eavesdropping on or intercepting telephone calls. If the interception were such as to constitute a criminal offence, then the information would surely have been obtained unlawfully. It seems an unavoidable conclusion that there would be a breach of the first data protection principle.

3.3 On the other hand there may have been no criminality, merely surreptitious or under-hand behaviour. In such a case, the Registrar would wish to consider whether the information had been fairly obtained and the data subsequently fairly processed. Regard should be had to the decisions of the Tribunal and to paragraph 1 of Part II of Schedule 1 of the 1984 Act referred to earlier. Such a case may well amount to a breach of the first data protection principle probably by the unfair obtaining of information.

27 November 1997]

[Continued]

3.4 Eavesdropping on a telephone conversation as described in para 3.2 might also give rise to a duty of confidence which would be breached by unlawful subsequent publication.⁸ Processing in order to effect the publication would then, in the Registrar's view, become unlawful and therefore a breach of the requirement of the first data protection principle that personal data should be processed fairly and lawfully.

3.5 The Registrar has not received any complaint against a newspaper relevant to these issues. She need not act only on receipt of a complaint—and does indeed pursue matters of general significance that come to her notice—but she is reluctant to intervene in the personal affairs of individuals, if they have not invited her assistance. Consequently, the previous suggestions can only be speculation about how the Registrar would react when considering the circumstances and merits of any particular case.

4. THE DIRECTIVE

4.1 In the summer of 1990, the Commission of the European Communities published a proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data (SYN 287). That draft directive was finally adopted on 24 July 1995 and published in the Official Journal on 23 November 1995 as Directive 95/46/EEC. An objective of the directive is to harmonise data protection laws in the Community at a high level of protection for individuals and, in particular, to ensure that the protection given by current legislation in individual Member States is not diminished.

4.2 The substance of the Directive is drawn from the Council of Europe Data Protection Convention (Treaty 108)⁹ and follows the general principles which can be found in both the UK data protection legislation and other European legislation. Some elements—such as those relating to sensitive data—are stronger than in the 1984 Act, but much of the ground is entirely familiar. Of some significance might be Articles 22 and 23 of the Directive which give individuals a right to a judicial remedy and compensation for any breach of the substantial data protection rules. By comparison there are very limited rights under the 1984 Act for individuals to sue for their own remedies. Notable amongst the differences is the express requirement in Article 9 for some balance to be struck between privacy and freedom of expression.

4.3 The text of Article 9 of the Directive reads thus:

“Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.”

4.4. The article sets the objective of the exemptions as (and probably restricts them):

“... to reconcile the right to privacy with rules governing freedom of expression”.

The whole article is founded on the footing that there is a right to privacy.

4.5 This emerges more strongly from Article 1(1) of the Directive. It runs thus:

“In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.”

It is readily apparent from Recitals 10 and 11 that the right to privacy is the right to private life found in Article 8 of the European Convention on Human Rights (ECHR)¹⁰ and that the Directive owes its principles to that and to Treaty 108.

4.6 The Directive is clearly privacy legislation and Article 9 must be seen as limited authority to circumscribe privacy rights in order to protect the right to freedom of expression in the context of journalism and artistic and literary expression. That seems tolerably clear from the formula used in the article:

“Member States shall provide exemptions . . . only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.”

If there were any doubt, reference to Recital 37 of the Preamble should remove it. There an express reference is made to Article 10 of the ECHR which declares the right to freedom of expression; the need to balance different fundamental rights is also clearly stated. But the Recital makes it equally clear that there should not be complete exemption from data protection control:

“... whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing: whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, eg to publish a regular report or to refer matters to the judicial authorities.”

⁸ cf the taking of photographs surreptitiously, described by Laws J in *Hellewell v Chief Constable of Derbyshire* [1995] 4 All ER at p. 475d.

⁹ Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series No. 108 Strasbourg 1981.

¹⁰ Council of Europe Convention for the protection of human rights and fundamental freedoms European Treaty Series No. 5.

27 November 1997]

[Continued]

4.7 It is still left to Member States to strike the balance between privacy and freedom of expression. Considerable margin of appreciation is available. It must be remembered, however, that the starting point in the United Kingdom is that there is no special exemption from data protection for journalism and that individuals have the right to expect publishers and broadcasters to comply with the Data Protection Principles as they are bound so to do by the 1984 Act. Any removal or weakening of that duty is a removal of privacy rights already granted by the United Kingdom law.

5. CONCLUSIONS ON THE IMPLEMENTATION OF ARTICLE 9

5.1 It is not clear to the Registrar which elements of privacy protection afforded by the Directive might unreasonably restrain freedom of expression. A distinction might be made between ordinary individuals and those who have placed themselves in the public domain—eg politicians. There might be a need to exercise care over the imposition of prior-restraint on publication. Perhaps subject access is a problem in the case of legitimate investigative journalism. Perhaps the extended right of individuals to pursue their remedies in the Courts will be a novel difficulty. These and other matters will need to be assessed against the policy established by Treaty 108 and the Directive permanently moving the goal-posts of society: namely, individuals are now entitled to knowledge of what information is held about them and to a degree of control over that information unless good cause can be shown to the contrary.

5.2 The Registrar would now like to see a careful examination of journalistic activity (and for that matter work of artistic or literary expression) with a view to identifying the problem areas. Those activities could then be tested to identify any need to cut back the existing and prospective protection of privacy in order to reconcile that protection with freedom of expression. On the basis of the information already gathered by her Office, the Registrar would expect to see a re-examination of proposals for a public interest defence for publishers and journalists and a revisiting of other ideas discussed in recent public debate in order to ensure a sound footing for the application of Article 9 of the Directive in new legislation.

30 May 1996

Examination of Witnesses

MRS ELIZABETH FRANCE, Data Protection Registrar, and MR JONATHAN BAMFORD, Assistant Data Protection Registrar, called in and examined.

Chairman

222. Mrs France and Mr Bamford, thank you very much for coming to see us. Thank you, first of all, also for the written evidence which you and your staff have submitted which has been very helpful. We much appreciate that. This is an opportunity to explore policy issues rather than the technicalities (and I know that is in line with your own thinking) but nevertheless new digital technologies do raise a number of important policy issues and particularly we are interested in your experiences with CCTV surveillance systems. The normal approach, as you probably know, is for you, if you would like to, to make any opening remarks. We then have a number of questions and supplementary questions. Have you any opening comments you would like to make?

(Mrs France) Yes, indeed. Thank you very much for the opportunity to give oral evidence to the Committee. We are very grateful for that chance. Perhaps I could open by saying a little bit about the history—very briefly—of our involvement in this sort of technology and where we think it is going. We have had on the statute book a law relating to data protection since 1984 based on a 1981 Convention. You will appreciate that, when Parliament was looking at legislation in 1983/84, it had no conception of the state of the use of new technology that we find ourselves confronted with today. But the saving grace of that 1984 legislation is the fact that its draftsmen kept it high level with no specific reference to specific types of technology. I would encourage the Committee to avoid specific references to technology in legislation for the reason that, as soon as the ink

is dry, the references are irrelevant—or in danger of being so. One of the advantages we have had in interpreting the 1984 Act is that it talks about automatic processing; it does not even talk about computers, so we have been able to interpret it fairly widely and it has allowed us to have some involvement in issues such as the development of CCTV (though not to the extent that we would like) and we hope the changes in the law which are imminent will allow us to have a greater involvement. Might I perhaps at this point explain that we have an EU directive which was adopted on 24 October 1995 which has to be incorporated into domestic law by 24 October 1998. The Government has agreed to do that by primary legislation and it is my understanding that there will be a Bill before your Lordships' House before the end of the year. Now that Bill gives an opportunity to look at some of these issues; its heart is the same as the heart of the 1984 Act. The principles at which the Committee has looked in the 1984 Act will still be found in the new legislation. The differences are in breadth of interpretation. The Directive's definition of processing, is far broader than the 1984 Act definition and certainly includes anything you can imagine doing with data. The Directive's definition of personal data is broader than the 1984 Act and one of the limitations we have in looking at CCTV, for example, is that the 1984 Act requires processing to be by reference to an individual. It is not a matter for us of whether the technology is analogue or digital; it is a matter of the sophistication of the totality of the equipment because you could have a swipe card with an

27 November 1997]

MRS ELIZABETH FRANCE AND MR JONATHON BAMFORD

[Continued]

Chairman *contd.*]

analogue CCTV system which would allow you to process by reference to an individual but, more often than not today, the present technology means that CCTV systems are not processing information by reference to individuals. That means that we can only offer best practice advice but do not have scope to enforce the Principles. We would expect that to change with the definitions in the new law. The other area of the new law, before I stop the introduction, that we think might be of interest to the Committee is that whereas the present law allows me to encourage codes of practice, the Directive and the Government's proposals for the new law talk about codes of conduct and actually allow the supervisory authority (that is currently my office) itself to introduce codes of conduct which can be used as a base line for using the powers of enforcement that Parliament then gives. That is a change from the present law and might be useful in this context.

223. That is very helpful. If we could stick with CCTV surveillance systems, of course we have heard a lot about them in city centres and elsewhere and you have already touched on this in your written submissions. I think it would be helpful if you could outline your role in the protection of privacy of individuals insofar as it relates to the CCTV systems and tell us how, in general, CCTV surveillance fits with the principles that data should be obtained and processed fairly and should not be excessive?

(*Mrs France*) With the present state of the technology and restrictions in the definition of the law, what we have sought to do is encourage the adoption of the Data Protection Principles as a voluntary basis for codes of practice where CCTV is used. Jonathan Bamford has done a lot of work with local authorities and with the police in developing codes of practice and he could certainly explain to you our practical experience of trying to encourage people to use those codes of practice. But that is as far as we can usually go at the moment given the state of technology and the restrictions in the law.

(*Mr Bamford*) We do use the basic eight Data Protection Principles as a backbone on which to build the code of practice which starts from the obtaining of the images and the need for notifications, not only whether CCTV surveillance is taking place but who is actually undertaking the surveillance because that is not always obvious to the public. They may think it is the town council or the police but actually it might be a private organisation—a shopping centre or something like that. The code goes through then to what happens with the images in terms of how they are processed; would it be right that images captured on a CCTV town centre scheme are made available, say, to the broadcast media for more general view. We have certainly taken the view that there might be arguments that that is unfair processing within the terms of the Data Protection Act. Then it goes through to issues about the extent of the images; should they comply with the Fourth Principle in terms of data not being excessive or irrelevant and limitations on the field of view, perhaps, of cameras of residential property where that is not really the purpose of having them through to how long the data is held for, and security and those sorts of measures.

So we tend to build the codes around those basic facets that are there in the Data Protection Act, essentially designed to protect people from the misuse of data.

224. Are there any organisations which operate CCTV systems, apart from the police, registered with you?

(*Mrs France*) Yes, indeed. Anybody in the United Kingdom processing personal data automatically is required to register with us. Clearly, as I have already said, if they are not processing by reference to individuals then they would not, under the current law, need to register but as far as we are aware the sorts of organisations operating CCTV schemes are organisations who are processing personal data for a range of reasons. We have not come across any such bodies not registered with us.

(*Mr Bamford*) One of the difficulties that we have in terms of answering the question who is registered for this and who is not is that data users register the general purpose for which they process personal data.

Lord Howie of Troon

225. Those codes of practice are presumably voluntary?

(*Mrs France*) They are at the moment. They will continue to be voluntary under the changes we expect to see in the law. Let me make clear that, under the present law, my ability to satisfy the concerns of this Committee would be extremely limited. My hope is that the changes in the law, although not extensive, just shift us to the point where some of these issues can be addressed and one of those is that although codes of conduct, as they are called in the Government's proposals, are still voluntary there is an ability for my office itself to introduce such codes. That is new. So I could issue a code of practice relating to CCTV and I could then use that as the base line for deciding whether to take enforcement action to enforce the eight Data Protection Principles, as they now are. I am not sure how they will be drafted in the new legislation.

226. So if people do not follow the code of practice, you can enforce it?

(*Mrs France*) Not currently but I hope to be able to once there has been a change in the law.

Lord Ackner

227. How can you do that? It is still a code of conduct.

(*Mrs France*) Yes. Can I refer to the powers I have under the 1984 Act because it is difficult for me to be sure how Parliament is going to frame my powers? I have seen the Directive, of course, and that has to be incorporated so we have a reasonable idea of what the new law is going to look like. At the moment there are areas where codes of practice exist. We have a code of practice with the Association of Chief Police Officers relating to their retention of personal records. We have other codes of practice drawn up, for example, by the Justices' Clerks, so we have those areas where codes of practice have been drawn up

27 November 1997]

MRS ELIZABETH FRANCE AND MR JONATHAN BAMFORD

[Continued]

Lord Ackner *contd.*]

which are owned by the group who have drawn them up; they bring them to me and ask me if I think they are acceptable. Mr Bamford has worked very closely with groups in the criminal justice area who have drawn up codes of practice—as we call them—under the 1984 Act. I then have powers administratively to enforce the eight Data Protection Principles. If a registered data user breaches a principle, then I have power to issue an enforcement notice either to tell him to desist from the practice; to delete his records; amend them—it depends what the issue is. That is a power which is appealable to the data protection Tribunal. That tribunal sits rarely because our practice is to try and achieve compliance by agreement rather than by enforcement but it does sit—indeed it is sitting for a preliminary hearing this morning—and once it has taken a decision, the data user either complies with that decision or it can appeal through to the courts, but any breach of an enforcement notice that has been endorsed by the Tribunal or is not appealed is a criminal offence.

228. I follow that, but I still do not follow how you establish a breach of one of the principles by reference to the code of conduct unless the code of conduct merely repeats the principle.

(Mrs France) It embellishes the principles.

(Mr Bamford) I may be able to help you because my role is really in trying to ensure that the various sectors who have codes of practice which cover them actually comply with those. In terms of the standards set in the code, and the Registrar has referred to the Association of Chief Police Officers' code of practice, we have some very detailed rules about the retention of police records. If the Registrar receives a complaint from an individual who is concerned that their data has been held longer than it should be, because the Sixth Principle says that personal data should not be held longer than necessary for the purpose, one of the things we will look at in trying to determine whether the retention period is correct is that benchmark set down in the code. We will look at that and see whether that standard has been adhered to. It is not binding but it informs the Registrar's judgment then of what would be the norm for data of that particular ilk. Often, in our discussions then with that particular data user, the fact that there is an industry standard or a code with a particular provision in it is quite persuasive and that can be very helpful in terms of them taking action to ensure compliance with the Principle—short of us having to resort to enforcement action.

(Mrs France) What you could say is that codes of practice under the present law and codes of conduct under the new law, as we expect them to be, are a way of us turning what is largely a reactive set of powers for the supervisory authority into a proactive ability to set standards. So while normally, we can only take enforcement action once we have a complaint in front of us, sitting down with data users and trying to develop codes, we try and anticipate complaints and put some flesh on the bones of the Principles in the legislation to apply to a particular sector. That could be direct marketing or policing, charities work or credit referencing; we cover the whole range. So the Principles as contained in primary legislation will never be detailed enough.

Lord Nathan

229. I want to pursue the question of whether you are correct in being satisfied that you know those who are operating CCTV. Evidence given to us indicated you could start with police surveillance of streets and so forth, as in the city of London. You then get on to privately owned shopping centres run by some organisation; you then get into the shops—Marks & Spencers and so forth, Barclays Bank, those two were mentioned—but you also find (so I am told) that you get into a newsagents which is quite a small affair. I saw a shop in Hove which advertised that it was supplying CCTV equipment and somebody mentioned to me that they did and they were very good but that it was frightfully expensive. This was a small shop. Are you satisfied that people in the small shops are informing you? Also, I am told that there is some surveillance of work being carried out in garages and, indeed, in open plan offices. It seems to be very widespread so I thought I would pursue it with you.

(Mrs France) Yes. If they are using CCTV in the way you suggest and are not doing any other processing of personal data then, under the present law, they would not be required to register with me because they would not be processing by reference to an individual. The larger organisations using CCTV cameras are processing personal data for other reasons. Therefore they are registered data users. So that, for example, all the banks will be registered with us in any event so we can look at the way they process the totality of their personal data. Registration under the Data Protection Act does not pull out particular ways you process information. They would not have to specify that they were using CCTV. One of the other things we need to look at is the fact that there is a universal requirement under the present law to register which we accept is not applied fully. We do not have the resources to go and make sure that every newsagent is registered. Under the new law I am pleased to say that universal registration would not be a requirement and the notification requirement in the Directive need only apply in certain circumstances. My understanding from the Government's proposals and from the responses I have made to the Home Office suggest that notification will only bite on those whose processing causes some degree of risk to the individual. But whereas under the present law I can only use my powers of enforcement against registered data users, under the forthcoming legislation those powers of enforcement will apply wherever there is a breach of the Principles regardless of whether notification was required. In those cases, if the corner newsagent were to use CCTV in a way that breached privacy, even if they did nothing else that caused a problem, if a complaint were made to me I would be able to look at it but I would still be relying on complaints being made.

Lord Flowers

230. Mrs France has already touched on the question I wanted to ask in her very interesting opening statement but I will pursue it nevertheless. Most image systems including CCTV, whether they

27 November 1997]

MRS ELIZABETH FRANCE AND MR JONATHAN BAMFORD

[Continued]

Lord Flowers *contd.*]

are digital or analogue it matters not, are capable of having digital technology applied to them in order to modify in some way the image—perhaps legitimately to enhance it or something, or perhaps not so legitimately. Does the Data Protection Act apply to such activities as that? If it does, how may it be enforced and if it does not, why not?

(*Mrs France*) This is to do with what we would call the fair processing provisions in the current legislation. Whether we are talking about image or word, any amendment to a record which then creates an unfair situation for the individual would be a breach of the Data Protection Principles but I have to take you back again to my limitations; that a lot of this processing is not caught at the moment at all because of the fact that the processing is not by reference to an individual. I am sorry to keep having to go back to that but that is one of the fundamental weaknesses of the 1984 Act in relation to what we are discussing.

231. If we are talking about what the police do, looking at motor cars and who drives them and the number plate and so on, that is a reference to the individuals being the owners of the car.

(*Mrs France*) If they store it in a way that allows them to extract it by reference to a car number or to a name, then it is caught. For instance, I went round and to look at broadcasters' uses of editorial suites and CCTV and various means of capturing images and you had still in some ways very basic technology, much like my video at home, where you knew which tape it was on and how many seconds into the tape you needed to go to find the image you wanted. That is not automatic processing by reference to the individual. On the other hand, they showed me some technology which allowed them to key in somebody's name or what somebody was wearing and the right image would come up on the screen. That is processing by reference to an individual. So at the moment whether something is caught or not is purely a matter under the 1984 Act of the sophistication of the technology. That, I hope, is one of the big changes which will occur later this year or beginning of next when we have incorporation of the EU Directive. I can only look at the definitions in the EU Directive, but they would do away with that problem because they talk about a person being able to be identified directly or indirectly from information that is held and, as I say, the definition in the Directive of processing is very broad. I trust that when the Bill is before your Lordships' House you will check the definitions are similar to those in the Directive.

Baroness Hogg

232. In your last answer you have effectively answered a question we were going to come to on the extent to which powerful data matching technologies would be caught. It seems clear to me it falls under your definition of level of sophistication. What I am not clear about, however, in relation to that last point you made is what the real meaning is of this phrase "unfair use of"?

(*Mrs France*) The Principle is fairly broadly drawn. It is in Schedule 2 of the current Data Protection Act and really it is a matter of

interpretation. What it actually says is: "The information to be contained in personal data shall be obtained and personal data shall be processed fairly and lawfully". That is all it says. So the interpretation over the last thirteen years has been a matter for my predecessor and myself. We have taken very few cases to the Tribunal and so there is very little case law. We have been left to interpret—with the co-operation in most cases of data users—and we have developed guidance and guidance notes which are available to data users.

233. Following that up, has that led you in the direction of interpreting "fairness" as a process word, whether the data had been fiddled or enhanced or whatever, or the uses of, for example, data?

(*Mrs France*) No. We put ourselves in the position of the individual in looking at fairness and we ask whether the individual has been caused any unfairness by the way the data has been stored, held, or used.

234. And whether it is an invasion of privacy in unfairness?

(*Mrs France*) Yes.

235. How does it relate to that and, if so, how is that defined as "fair" or "unfair". Is it just doing it?

(*Mrs France*) It is a combination. You have to look at the processing in context. You have to look at expectation; you have to look at consent; you have to look at the relationship between the person processing and the person about who the processing is done. It varies enormously in different contexts.

(*Mr Bamford*) There is a little bit of case law in this area in terms of unfair processing. It is obviously terribly subjective. Really the Data Protection Tribunal which is the appellate body against the Registrar's enforcement decisions involving people has looked at this issue of unfairness in the past and has really looked at what the consequences are for an individual for the processing and what the actual effects are in real terms for an individual and whether they suffer some detriment or something like that. It is made clear really in looking at these sorts of matters that the interests of the individual are paramount. They are not the only consideration; there may be counterbalancing features but they are certainly paramount so what is the consequence for that individual over processing that has taken place? Would that amount to some form of detriment or other consequence for the individual?

(*Mrs France*) This, again, is all strengthened in the EU Directive which gives much clearer rights to individuals to go to the courts if they feel they have suffered distress or damage as a result of the way information has been processed. At the moment there is a limited right to do that. It was in action that my predecessor took against the credit reference agencies that the Tribunal issued some of its understanding of the term "fair processing", but you will understand that you have to look at it in the context. If I am walking down a street in a public place and I am made aware that I am being filmed it might not be an unfairness if that is not used for any unexpected purpose. It might become an unfairness if, for some reason not related to my behaviour in the street, that image is used for some other totally

27 November 1997]

MRS ELIZABETH FRANCE AND MR JONATHAN BAMFORD

[Continued]

Baroness Hogg *contd.*]

unrelated purpose. There might be other circumstances where I am being covertly filmed where the very fact that I am being filmed is itself an unfairness. So you have to look at the context.

236. We have an example of the use of face recognition by immigration authorities which I thought had wonderful language: "Face recognition can be performed passively without requiring the participation of the subject."—that seems to be a wonderful euphemism for consent or knowledge—"and is particularly useful where active participation of the subject is not possible". This is used by a public authority so I suppose—

(*Mrs France*) Yes. If that was used by a public authority, I will say this you will appreciate off the top of my head: my immediate reaction would be that a public authority doing that either requires unambiguous consent or the law to allow it to do it. Quite often with public bodies, and we have said it recently, departments must go back to Parliament and say "This is something which public order or the prevention of crime requires that we do". Then it is transparent. All right—it may be not transparent to the individual at the moment it is happening but it has been through the Parliamentary process.

Lord Ackner

237. The Act in fact in the second Schedule gives you some assistance because it deals with the interpretation and, for instance, in regard to this question of fairness, it does say that, "subject to subparagraph (2), in determining whether the information was obtained fairly, regard shall be had to the method by which it was obtained, including in particular whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed". That takes you quite some distance, does it not?

(*Mrs France*) Yes, it does.

Bishop of Leicester

238. We are still in the area of the interest of individuals and obviously we are aware of the possible benefits of the CCTV surveillance systems in public places, shopping centres, football grounds, etc. But we have also heard suggestions that they can be used to track and even exclude what is regarded as an undesirable individual. If that is the case, what right of access do you feel the public should have to images of themselves that have been captured by these systems?

(*Mrs France*) Let us assume these systems, because of the sophistication described, are caught by the Data Protection Act now and certainly will be in the future. In that case we would expect full subject access to information held about you. That is, you should be able to see everything that is held about you except in some very limited circumstances: for example when providing you with that information would inhibit the prevention or detection of crime, and even that has to be on a case-by-case basis. You cannot say that surveillance is generally available to prevent crime therefore no access is available to anybody.

239. If I turn up at Leicester City football ground and I am excluded because I have been captured on film causing trouble three months ago, I should be able to demand the opportunity of actually seeing the image and responding to it?

(*Mr Bamford*) Essentially yes, you would have to be given a copy of the data and the images as such unless to provide them would be "likely to prejudice" (is the test in the Act) the prevention or detection of crime or the apprehension or prosecution of offenders. Clearly there may not be satisfaction of that test of "likely to prejudice" if you are fully aware of the reason why you have been excluded and it would not necessarily prejudice that. Where there can be issues around this is the extent to which any third parties who are also caught on those images should have their images in some way blurred so they are not identified when you are given access to the images relating to yourself.

(*Mrs France*) One of the things we are concerned to ensure remains in the new legislation is that that ability to blot out third parties is, if you like, a requirement and not an excuse. You do not say "I cannot give you the image because it would reveal third parties". If people are putting sophisticated systems in place then they do it knowing the legal background against which they are installing them and if they are capable of matching images then they should also be capable of blurring out surrounding images if they only want to give you the image of your own action.

Chairman

240. That would be acceptable, would it?

(*Mrs France*) As far as we are concerned. Our interest is in protecting the right of the individual, the individual's right to privacy, and that has to have two sides to it. Your right to see information about yourself is part of your package of rights. It may sound odd to say your right to see what is held about you relates to your right to privacy but, in order to have some control about what happens to information about yourself, you must be able to see it. At the same time it is our duty to protect the rights of others whose information might be captured and not give you that information. There may be other reasons you could be given it but, under data protection legislation, we would expect you only to see information relating to you.

241. That does seem to exclude partly the context.

(*Mrs France*) You would see the actions. On a clip of film you would see the actions but you would not be able to identify the individuals. There would be sufficient blurring of images that you would not be able to identify from that who else was there. There might be other reasons; you might take court action leading to you being able to see the whole thing but, under data protection law, you would only be able to see your own images.

(*Mr Bamford*) Basically the Act's subject's access rights—the right of access that we all have to information held about us on computer—do allow the data user to withhold details relating to third parties unless the individual has consented to disclosure. But it essentially says "They may

27 November 1997]

MRS ELIZABETH FRANCE AND MR JONATHON BAMFORD

[Continued]

Chairman *contd.*]

withhold". It is not a requirement to necessarily withhold. To use the example of the trouble at a football ground, clearly it might not be sensible, if it is Leicestershire Constabulary who have these video tapes, for them to blur out the details of the officer arresting you if you appear there because that might be something which is very well known to you because they actually gave you the details of them, but the unassociated third party who happened to be sitting behind you in the stand might be something there is more of a concern about and you might blur out the face of that particular person.

(*Mrs France*) We are saying the basic rights in data protection legislation which have been there and will continue to be there for the individual to see anything that is held about them if it is automatically processed should remain regardless of the technology. If we are capable of using more sophisticated technology, then we are capable of meeting that requirement.

(*Mr Bamford*) The Act really should provide as much information as possible without revealing the identity of other parties. In the case of a person sitting behind perhaps it would just be the face but it should just be the minimum amount necessary to maintain the anonymity of that other party.

Lord Howie of Troon

242. Let us forget about third parties for the moment and go back to the Bishop who has been photographed at Leicester City football ground where no doubt he is going to give comfort to the goalkeeper. In the earlier answer, he seems to have been told they had this photograph but this photograph was taken some weeks previously perhaps and is on record for some time. What access has he got to that picture before he turns up to the ground and is then turned away?

(*Mrs France*) There is always this difficult question of needing to know something is there in order to ask to see it, but provided you do know there is a chance that an authority holds any personal information about you, you have a right to ask to see it. If you have any reason to believe that to be the case, then you can ask to see it.

243. What I really mean is this: the image is presumably held because the Bishop is starting to be a suspicious character in some way. Would it be a good idea if he were told this image was held and he would then have access to it to see if he, in fact, were a suspicious character?

(*Mrs France*) This relates to all sorts of police held data so I will ask Mr Bamford to answer.

(*Mr Bamford*) Yes. In reality it is no different from the police obtaining covert information and intelligence generally. There is a provision in the Act which says the police and other law enforcement bodies who are obtaining information for the prevention or detection of crime, and where it would be likely to prejudice those matters, if they give the normal standards of notification, do not actually have to comply with that standard. So they would not actually have to make people aware this was happening if it would be prejudicial to the crime prevention purposes and so on to do that.

244. So you are saying the range of access is somewhat limited?

(*Mr Bamford*) From practical experience of dealing with the police over more general information, they do tend to be very careful in terms of when they would rely on exemptions from the right of access and they do take this very seriously. You can imagine that we encourage them to do so. We do stress this test of "likely to prejudice" in a particular case to give access.

(*Mrs France*) I repeat the law only allows that test to be applied on a case-by-case basis. So at any time when you ask for access to your information, unless revealing that information would prejudice a current enquiry (and clearly the police must draw their own boundaries round that), simply because it was obtained for intelligence purposes is not a reason not to disclose it to you.

(*Mr Bamford*) There has been some case law on this as well in terms of the Data Protection Tribunal in the *Equifax* case which makes clear that this "likely to prejudice" (which obviously is open to interpretation) is not "might conceivably prejudice"; that there is a real likelihood of some crime prevention matter being prejudiced by giving access in this particular instance.

Lord Ackner

245. If I want to establish an alibi and I believe that the police have got material which positively or negatively will assist me and the police say "No, we do not provide this sort of information", can I get any assistance through you or do I have to go to the courts for a sub poena?

(*Mrs France*) If the information you require is information they could provide to you under Section 21 of the Data Protection Act, then the purpose for which you want it is immaterial. If it is information about you and they hold it and it would not prejudice the prevention or detection of crime to let you have it, they are required to give it to you.

246. And if they will not?

(*Mrs France*) Then the action is to the courts.

(*Mr Bamford*) You have an individual right to take action to the courts or you can complain to the Registrar that is it in breach of the Seventh Data Protection Principle—in those instances people complain to the Registrar—and then we have power to investigate these matters. There has been a number of cases—not with CCTV images—where, as you can imagine, people have made subject access requests to the police, believe the police have more information than they are actually revealing to them and they complain to the Registrar and we investigate and find out what the police are holding on computer and whether they have correctly relied on any exemption.

(*Mrs France*) There are some current limitations to our powers to have a look at what is held by data users. We can go to courts for warrants in certain circumstances but under the 1984 Act we rely on the co-operation of the data user more than I would like in making sure we see that information. Again, we hope that will be remedied in the new law where the Government's proposals refer to some form of information notice power, but I do have to say to the

27 November 1997]

MRS ELIZABETH FRANCE AND MR JONATHAN BAMFORD

[Continued]

Lord Ackner *contd.*]

Committee that we can only say we see information and we hope we are having the co-operation of data users. We are confident we normally do get their co-operation but our powers to insist are limited.

Baroness Hogg

247. There is one issue about the range of your responsibilities and activities that I would just like to ask you about. The amount of information that is held or processed electronically has, of course, been transformed since the 1984 Act. I am not quite sure where some of these boundaries now rest. For example, in 1985 I was working for *The Times* when it transferred itself to electronic inputting. There was a sudden flurry of panic in *The Times* as to what would be the effect of switching its databank of obituaries on to electronic systems; whether Members of this Committee would turn up at the door of *The Times* and ask to see what was held by them. Does the Act provide this power and is this creating problems, given that almost all written material is now held electronically in some form or another?

(*Mrs France*) The answer to that is an interesting one because the 1984 Act made no exemptions for artistic or journalistic purposes at all. Therefore I could apply the law to the media in the way you suggest. However, as I have said, I respond to complaints. I am not aware of anybody making a subject access request for their obituary and being refused. They certainly have not come to me about it. There is no doubt that, under the present law, there would be no exemption applying. We have been trying to explain this to the media recently because it seems to us that the 1984 Act could well cause some problems as we go further into the electronic age. Most of their newspapers appear in electronic format which allows you to search by reference to a name. A lot of their images are digitally enhanced—sometimes properly but nevertheless there is processing involved there in the creation of images. We have said we think it perfectly proper that the new law should have a clear exemption for journalistic and artistic purposes. Indeed, we have no choice because Article 9 of the Directive says that, but Article 9 of the Directive which has to be incorporated says that that exemption for artistic and journalistic purposes should only be such as is necessary, and I quote: “Member States shall provide for exemptions or derogations from various provisions of the Directive for the processing of personal data carried out solely for journalistic purposes or for the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression”. I think that is going to be an interesting test—

248. Good money for lawyers!

(*Mrs France*)—but the fact remains that, under the 1984 Act, there are no such exemptions so, strictly speaking, anything that is held—for whatever journalistic purpose—if you can access it by putting a name into the system, then that named person has a right to a copy of it.

Chairman

249. But you do talk in one of your very helpful written pieces about the Registrar certainly having “concerns about data-matching for journalistic purposes”. That is paragraph 2.12 at the bottom. You say you doubt “whether journalists are currently matching information by the technical interlinking of files and running one against another, the technology is readily available, and the Registrar would certainly have concerns about data-matching for journalistic purposes.”

(*Mrs France*) We do have general concerns about data-matching in all contexts. It is one of the technologies of today and although some jurisdictions elsewhere have looked at referring to data-matching in their law, it is another area where I think a code of conduct which is adaptable would be preferable to reference to data-matching in the law because it is simply a technique that is being used which matches information either within the same database or between databases looking for common features and they do not have to be images—they can be pieces of information. We have expressed concern about some of these uses of data-matching across a wide spectrum of activity, most recently during the passage of the Social Security Administration and Fraud Bill where we looked for an undertaking from ministers to produce a statutory code of practice. In fact, what we received was an undertaking to produce a voluntary code; that undertaking is being picked up by present ministers and we wait to see the draft, but the whole area of data-matching raises concerns for us.

Baroness Hogg

250. Data-matching certainly is a standard journalistic practice now.

(*Mrs France*) Yes. It is certainly going on; it is a matter of making sure there are some rules to go with it. Mr Bamford has been involved in working with the local Government Audit Commission who have just published their own code of practice setting out guidelines for data-matching.

Lord Kirkwood

251. Without going into the details of authenticating images and documents, I would like to ask about the business of technology and encryption. I would like to hear your general views on the need for individuals to protect data by encryption which probably has the beneficial effects of establishing the authenticity in court. Do you think the Government should do more to encourage technologies for watermarking, digital signatures and the rest? In particular I was impressed or I noted a comment in your written evidence saying “Any new law at this stage should give incentives to develop valuable techniques without prescribing a specific solution”. That seems a very important principle. As you have said before: prescription is always overtaken by new technology and if you can frame these things in the form of general principles that is a much better way of doing it.

27 November 1997]

MRS ELIZABETH FRANCE AND MR JONATHAN BAMFORD

[Continued]

Lord Kirkwood *contd.*]

(Mrs France) It might be interesting for the Committee to be aware that we have a fairly close-knit community of data protection and privacy commissioners worldwide and we are all, as you would expect, facing the same sorts of issues. One of our current pleas on any national or international platforms is for encouragement of development of what we call privacy enhancing technologies. All of us have suffered from being seen by those who want to exploit new technologies as having some elements of ludditism within our offices. That is not what we are there to do. We are not there to say that new technology should not be exploited but that that new technology can be exploited without exploiting individuals if there is the will to develop, in parallel with the benefits that are immediately visible to business or law enforcement agencies, the techniques which allow privacy to be enhanced—whether by encryption, pseudonymous identities or simple things like hierarchies of passwords. You can use the technology to the benefit of the individual and then still get the best out of the technology. It seems to me that if electronic commerce is to get off the ground, if the Government's very proper push to see the delivery of Government services more cost effectively provided through the use of electronic service provision, then we have at the same time to push forward better use of encryption technologies for not just confidentiality but for authentication and validation of transactions. It is very important we push on with that as quickly as we can. We are very much in favour of the free market development of strong encryption methods. We support the OECD's recent guidelines and we are looking forward to seeing where the Department of Trade and Industry take their consultation on the possible establishment of trusted third parties and the wider use of encryption technology. It is important. We have to encourage (and we try to do this by working with some of the undergraduate bodies) software developers. We have been working with the British Computer Society and with some of the universities and with the software developers to try and encourage those developing systems to actually market this as added value to the sorts of systems we are talking about. Obviously some encouragement in that direction, by suggesting that perhaps the information produced would not be acceptable in some circumstances if these things were not built in, would be very helpful.

Chairman

252. You raise an interesting question in one of your submissions concerning the downloading of a whole database from a computer system in order to extract from it an element which is required for use by the courts. In that downloading, other individual's details may be affected. You identify it as a problem: could you expand on your thinking there?

(Mrs France) I think the problem arose because of the courts' interpretation and I think we quote the restrictive view taken in a particular case which I think was *Derby v Weldon*. The difficulty is that you will be seizing material beyond the scope of a traditional warrant partly because you do not know

what you are seizing but the importance of seizing a whole database is to have it and be able to look at its integrity and you need to seize the whole database and subject it to computer forensic expert examination in its entirety. I think we raise it as an educational point really; that you cannot use perhaps the traditional terminology and limitations of a warrant when you are talking about seizing electronic data. There is a danger and you do have to return the data fairly rapidly because sometimes you can put somebody's business in jeopardy. We seized under warrant the whole of a database of a business and obviously we had it looked at as quickly as we could to extract that information that was necessary for the court action. It is a new area, however, you do need to look at the integrity of the database as part of your examination of the material you have seized.

253. Does the new Bill which we have been talking about address this particular issue? It seems to me it is quite important particularly in the area which we have a strong interest in, the use of digital images in whatever form it is stored in courts.

(Mrs France) It is not an issue that is referred to in the Directive. Indeed the Directive itself does not extend, because of the limitations of the scope of EU Directives, to the criminal justice area but the Home Office took the decision and the Government took the decision to legislate through primary legislation so it would cover the criminal justice area. That means that while I cannot say what would be in the Bill there would be scope, if there was interest in doing so, to raise that during the passage of the Bill.

254. It clearly does cut very closely into your interest as a data registrar.

(Mrs France) Yes.

255. Could we look at getting a feel for how many complaints you receive each year from the public about data held by Government and commercial bodies?

(Mrs France) I can answer you in very general terms. Again, perhaps I can preface it by my making clear that, as a small grant-aided body, we are well aware that were we to canvass complaints, we would receive an enormous number more than we currently do. We can show that: a limited amount of advertising creates a huge increase in our mail bag, so we always have to make that point before giving you the figures. Last year we received 3,897 complaints in total. This year we are running already at about 20 per cent above that if we carry on at the same rate throughout the year. I cannot say we will reach quite that increase when the year is completed but certainly the figures are on an upward trend. The majority of those complaints is about the private sector. Year on year, since the office has been created, regardless of the total number of complaints, a third have always related to finance and credit matters. The complaints we get about the public sector are smaller in number but can be more complex to handle. Mr Bamford deals with the public sector and public sector complaints and I am sure he would endorse that.

(Mr Bamford) Yes. From past experience it can be quite complicated—particularly when you think about policing which we have touched on already this morning and issues to do with whether it is right

27 November 1997]

MRS ELIZABETH FRANCE AND MR JONATHAN BAMFORD

[Continued]

Chairman *contd.*]

for certain items of information to be held about people's intelligence data and matters like that. They can be very difficult matters to investigate and to come to judgments on and we spend a lot of resources on those sorts of matters. We do not receive a massive number of complaints but I think we have seen an increase in the last year, particularly in connection with criminal record keeping.

(*Mrs France*) We use our complaints as a trigger to look at the practice being undertaken and to make recommendations so it may only take one complaint to reveal to us practice we think should be amended.

Baroness Hogg

256. Is it very sensitive to television coverage of the issues?

(*Mrs France*) Yes, but I think what it is most sensitive to is clear confrontation with the effects of processing. People are aware of the amount of direct mail that comes through their door and they complain to us about it. People are embarrassed if they are refused credit in the High Street at the weekend for no apparently good reason and they complain to us. They are not necessarily aware of the effects of automatic processing quite so clearly and quite so immediately when it is done by public bodies. Having said that, the one body that we had an enormous number of complaints about, although we do not get so many now, was the Child Support Agency. We received an enormous number of complaints before my time relating to the Community Charge and the processing relating to that. Again, those are issues which are of concern to the public anyway and they then become aware of the processing problems relating to them. I think the more that Government decides to go down the road of electronic delivery of services, the more the public will seek some assurance that what they are told is happening to their information is in fact what is happening to it. When they are told there are virtual walls between information in different bits of Government, they will want to be confident that those virtual walls are in tact. That is another reason why we are seeking power, although I do not think it has found favour yet, to have some limited right to audit rather than to wait for complaints.

Chairman

257. The other point on this which I would be interested in is have you sensed that with the growth of the use of CCTV people are starting to ask for data on themselves from that? Have you sensed at any time public unease about the way that CCTV coverage is going and how much it has been used? Clearly those who use CCTV have a dual interest, one is the law enforcement and so on and the other is to maintain public confidence. What I am really looking for is any experience that you might have had in people approaching you which suggests that there is any falling off in public confidence about the way in which CCTV has been used?

(*Mr Bamford*) Perhaps I could answer that as somebody who heads the department that deals with the complaints that may come in from that direction.

I have to say that we have not received very many complaints at all about CCTV. When you speak to people and people want to talk to you about these sorts of matters there does seem to be an underlying recognition of concern but this has not manifested itself in actual complaints where somebody appears to have suffered as a result of this. We have only really dealt with one complaint which was in connection with one of these videos which were for sale containing certain elements of CCTV footage but that was very quickly disposed of in data protection terms because it did not fall within the scope of the legislation for the reasons we explained earlier on. We do not have many people beating a path to our door. What is encouraging is that we have many, many local authorities and others who are involved in this who actually are beating a path to our door to try and now put in place codes of practice and local guidelines to try and get some measure of safeguard for the public in their area. It is encouraging in many ways that what we are seeing are the people who may be seen as intruding trying to put in place some measures. Obviously we can encourage them in terms of best practice at the moment.

(*Mrs France*) CCTV is a very good example of the balance we face wherever we look. There is no doubt at all that CCTV not only is effective in crime prevention but also effective in reducing fear of crime and those are very important social objectives for any Government to want to ensure are put in place. But at the same time we do need to make sure that there are guidelines, that we do not stray so far that the confidence is lost in it and we then lose the benefits of crime prevention and prevention of fear of crime. We have always got a balancing act to do. It is very encouraging that the police and the local authorities have wanted to put guidelines in place from the outset. Once we see this technology squarely covered by new data protection law, although my powers to enforce will always be limited and we shall be looking probably at particular complaints and those will raise general issues, then I think we shall have gone a long way to make sure that that balance is properly kept in check.

258. So would you feel that a tick in the box from the Data Protection Registrar is helpful?

(*Mrs France*) Helpful. I thought you were going to say solves the problems! Certainly helpful. I think that having a code of practice instead of being simply voluntary, because we say it is not quite covered by the Data Protection Act, squarely under the Act will be helpful. It depends how important Parliament considers this sort of surveillance to be because, again, the Directive allows Parliament to determine certain categories of processing which require prior checking. This is a new concept, we have not had it before. Prior checking would mean that you could not begin the processing without the supervisory authority making some check as to the safeguards you have in place. The types of techniques to be included in prior checking, it is my understanding, will be included eventually in secondary legislation and I do not think, as yet, any full debate as to what sorts of techniques or types of processing will be included there has been undertaken.

27 November 1997]

MRS ELIZABETH FRANCE AND MR JONATHON BAMFORD

[Continued

Chairman *contd.*]

259. Any further questions? Thank you very much, Mrs France. Have you anything finally you would like to say before we call this to a close?

(Mrs France) No. I am grateful for the opportunity you have given us. Thank you very much.

Chairman] We are very grateful to you and to your colleague, Mr Bamford. Thank you very much indeed for coming to see us.

THURSDAY 4 DECEMBER 1997

Present:

Ackner, L.
Brain, L.
Craig of Radley, L.
(Chairman)
Hogg, B.

Kirkwood, L.
Leicester, Bp.
Nathan, L.
Phillips of Ellesmere, L.
Tombs, L.

Written Memorandum by IBM United Kingdom Limited

Thank you for your letters requesting IBM's position on the matters raised in the Call for Evidence before the Sub-Committee, and on the need for the Government to distinguish between the needs of national security and those of electronic commerce. I have also subsequently received some additional possible questions.

IBM is pleased to have been invited to respond and Mr Syd Chapman and I are happy to make ourselves available to attempt to answer any questions which the Sub-Committee may have. Mr Peter Stretton will accompany us as an observer.

I attach some outline responses to the Call for Evidence and the additional questions which may be of interest to the Committee.

QUESTION 1

What is the current and forecast future use of digital technology for image collection, storage and transmission?

IBM and its customers are at the forefront of the development of systems for the electronic delivery of banking, insurance, finance, manufacturing, distribution, retail, entertainment, travel, transport, and government services. Our objective is to help our customers serve the needs of their customers. The Hursley Laboratory located near Winchester has since 1958 been one of IBM Corporation's facilities responsible for the development of many significant hardware and software innovations within the Information Technology Industry including CICS, Message Queuing and Brokering, and Interactive Voice systems.

The scale of electronic commerce is undergoing a dramatic increase as network computing, the Internet, Intranets and the World Wide Web grow in importance. Computer generated digitised documents, spreadsheets, data, audio, video and graphic images, whether of still or moving pictures, are being collected, stored, transmitted, manipulated, compressed and enhanced at an ever increasing volume.

IBM has many customers throughout the world, including several government agencies in the Netherlands, Germany, and the United Kingdom, who have adopted image scanning technologies which enable them to discard original hard copy documents.

IBM considers that laws applying to electronic commerce and communications should be similar to and have the same purpose as the laws as they apply to physical commerce and communication. Certain limited amendments may be necessary to facilitate the use of electronic technologies where particular laws have the effect of preventing the use of these technologies. The Legislative Working Party of the Society for Computers and Law have recommended to the DTI in a Report on Digital Information and Requirements of Form that the Interpretation Act 1978 could be amended to import a definition of "writing" to include digital information and that "writing" be distinguished from physical writing on a physical medium. (see <http://www.qmw.ac.uk/ccls/itlaw/scldwp>). A similar approach is recommended for Scotland where legislative drafters are recommended to use the phrase "writing or an electronic equivalent" unless the intent is to restrict the transaction to words on a physical medium.

IBM welcomes the UK Government Direct initiative to promote the use by citizens of IT to access public information and services, and recognises the vital importance of ensuring and maintaining the confidentiality of communications and the role of encryption products and services in increasing the security and the perception of security associated with conducting transactions over electronic networks.

IBM believes that the adoption of digital technologies including digital imagery can provide great economic and social benefits. Although digital images are different from analogue images, they can have a probative evidential value equal to and in some instances greater than their analogue counterparts if the differences are understood and appropriate technical and procedural evidentiary preconditions are met.

IBM has responded to the proposals prepared by the DTI in March 1997 on The Licensing of Trusted Third Parties for the Provision of Encryption Services.

4 December 1997][Continued

IBM acknowledges the need for legitimate law enforcement agencies to continue to have the means to operate effectively and is working with customers, governments and industry associations across Europe to find a solution that meets the requirements of our customers and their governments.

QUESTION 1.1

What is its use by the courts and the legal profession?

The world wide market for optical storage products in 1994 was US\$ 3.1 billion and is expected to rise to US\$ 8.2 billion by the year 2000. The Home Office, the Law Society or the Society for Computers and Law may be able to provide details of the current use of digital technology by the UK courts and the legal profession. It may become appropriate for police interviews to be video recorded and some court processes conducted remotely.

QUESTION 1.2

What is the state of the art of image manipulation?

Digital images are one of many manifestations of digital information. They are merely datasets comprising machine readable code arranged in files which when displayed or plotted appear as visible images. They are not qualitatively different to other datasets such as voice, text or multimedia files although they are usually quantitatively larger than text files.

Digital images may be generated either by the scanning of conventional photographs or by Electronic Still Photography and Digital Video.

Commonly available Electronic Still Photography (ESP) digital cameras which use a Charged Coupled Device to write images directly to an incorporated computer hard drive as binary files and the associated image processing software products such as IBM's ImagePlus, and Adobe's Photoshop, enable the sophisticated manipulation of digital pictures and video images.

Access to the equipment and software that can be used to modify images is already widespread. The technology includes expensive, highly-sophisticated, still and video image editing suites of the sort that have been used to edit still images such as the controversial National Geographic cover picture of the Pyramids, or Time's picture of OJ Simpson and to edit video images for films such as "Terminator II" and Forrest Gump". It also includes consumer software that can be run on commonly available PCs, and which can place quite sophisticated image manipulation power in the hands of the amateur photographer for an incremental price of less than a hundred pounds.

Digital image manipulation is very powerful although considerable skill is needed to provide a convincing effect. Unlike analogue manipulation, the image may be changed at the pixel level, and once changed, there is no digital residue of the initial information. This can be contrasted with analogue manipulation, which may, in some circumstances, leave some clue as to the original image content. Digital image manipulation is so effective that it is possible to produce fake images that are virtually undetectable in their construction. (see George Bush/Margaret Thatcher images from Scientific American February 1994). Once produced, the process is impossible to undo to reveal what the image originally contained.

A digital image is not infinite in its information content; that is, the image cannot be magnified indefinitely to yield more and more detail. Neither can an analogue image, but there is a common misconception that somehow there is "more" information in a digital image than an analogue one. Digital images, if not captured correctly, will in general have less information in them than an original analogue.

A physical image exists in time, has a creation date, and ages through its life. All digital images may be re-created in physical hard copy form at any time and every re-creation is a new original. Digital images are qualitatively and quantitatively different from real physical analogue images. Real images are characterised by chemical processes (interaction of light with silver halide, interaction of water, suspended paint, particles and paper etc) which are inherently diffusion or concentration gradient driven. This means that these processes will yield transitions (from light to dark, from paper to paint) that are characterised by a diffusion length. This length is the distance over which the amount of one substance in or on another changes from a lot to a little. Although this length may be very small (oil paint or digital printers) to very large (water colours on paper), it is never zero.

With any digital image however the value of the intensity at any one point (a pixel) is unique, invariant, and the transitions are completely discontinuous from pixel to pixel. It is this "pixel uniqueness" and "isolation" that allows digital images to be manipulated so successfully, because once the value is changed, no residue of the previous value remains, and no magnification process can be used to look "between the pixels" to see whether the change has occurred. In the analogue world, falsifying images by bleaching or overpainting always leaves some region where the transition has not been correctly duplicated, and in this case more magnification can be applied to look at smaller and smaller effects.

4 December 1997]

[Continued]

It should be noted that two dimensional images are only one part of a much larger problem. Three dimensional, photo-realistic moving visualisations with real people in fictitious or altered landscapes are now possible and this extends the scope far beyond simple images. Just as a photograph is a convincing image, 3D moving visualisations can create totally convincing illusions.

QUESTION 2

Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean they should be treated differently when used as evidence?

In the absence of audit trail information which has been added to the data itself, at the time of its creation, it is often impossible to be sure that a digital image has not been modified, unless the modification itself shows artefacts.

However, IBM does not consider that difficulties of maintaining an audit trail are sufficiently significant to justify mandatory differential treatment when digitised images are used as evidence. Compliance with the best practice in respect of established and available security procedures, such as audit trails, terminal IDs, passwords and key stroke recorders as recommended by the BSI, should be a factor amongst others to be considered by a Court when assessing the probative value of digital images as evidence.

Digital images need not present qualitatively different legal difficulties to those presented by established reprographic technologies such as fax transmissions, photocopying or tape recording. The "presumption of regularity" ie that the machine (hardware and software) is working as designed, and that the images are authentic, does in practice usually apply unless there are compelling grounds to challenge this. In the US the Best Evidence rules and Business records exemption to the hearsay rule provided by the Federal Rules of Evidence 803(6), 901(b)(9) are the judicial basis for the operation of the presumption.

IBM supports the introduction of legislation which ensures the equal status of digital images as evidence if and to the extent that current law places greater weight on non digital evidence. The Danish Ministry of Research and Information Technology has proposed an Act on Digital Signatures, The Uniform Law Conference of Canada has issued a consultation paper on a Uniform Electronic Evidence Act and the US States of Utah, California and Washington have enacted or are in the process of enacting such legislation. It is recommended, however, that such legislation should avoid reference to specific technologies as far as possible in the light of the rate of technological change and the risk that the law will become obsolete in the event of technological obsolescence.

There are many commentators on the issue, including Douglas Goodin, an FBI Laboratory Special Photographic Unit Examiner, who discusses the issues of impermanence and the ease with which digital images may be altered. He distinguishes the two bases of image authenticity; maintenance of the original image file; and protecting the computer system from intentional or accidental compromise. He states that "an audit trail would provide an independent record of when the image was taken and anytime it has been altered from the original. It could possibly run as some kind of file comparison utility . . ." This would involve having to establish a centralized image storage and retrieval system within a given agency for the trail to have any meaning. Any software or data on an independent unconnected computer is pretty much at the mercy of anybody running it. (see www.trfsys.com/web/lynx/doug_goodin.htm)

QUESTION 3

Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence?

The use of fingerprints and other biometrics for identification and recognition as well as authentication techniques designed to place visible or invisible marks into digital images under secure conditions do increase the utility of digital images as evidence, by providing a reliable means of proving or disproving unauthorized manipulations. Although an altered copy of a digital image is no less original than the original data set from which it is derived, authentication techniques such as watermarking, IBM Cryptolopes (see <http://www.cryptolope.ibm.com/cryptolp.htm>), digital signatures and time stamping can form important aspects of an audit trail which can support or undermine the probative value of a digital image as evidence.

Watermarks are visible or invisible, robust or fragile, authentication codes, placed in a digital image, preferably during the capture process, to aid in establishing originality and detecting copyright infringement.

Watermarks may be characterised by the following descriptive terms:

Robust: able to withstand some image manipulations, and still be retrieved intact. Different schemes will be robust against different manipulations, depending where in the "signal" the watermark has been placed.

Fragile: retrievable after image manipulation, but demonstrably damaged by the manipulation. Good for demonstrating that an image has been tampered with.

4 December 1997][Continued

Visible: imbedded within the visually-perceptable part of the image, by, for example, altering the luminance of selected pixels.

Invisible: imbedded within some visually-imperceptible part of the image "signal".

The three most useful kinds of watermark are: robust visible, robust invisible and fragile invisible.

A robust invisible watermark will survive a limited amount of image processing, which may include cropping, compression and decompression, digital—to analogue—to digital conversions and scaling and skewing. A number of companies provide robust digital watermarking schemes for use particularly in deterring copyright infringement or proving that such infringement has occurred.

One example of robust visible watermarking is Visible Random Brightness Alteration—a technique developed by IBM Research in response to a requirement of the Vatican Library to enable Internet distribution of images acceptable for scholarly study but unacceptable for publication. The IBM Digital Library Website contains examples including the attached 16th century Aztec manuscript displaying the papal insignia as a visible embedded watermark. (<http://www.software.ibm.com/ls/dig-lib/vatican.htm>)

A fragile invisible watermark is more useful for authentication because if placed in an image, preferably at the time of capture, it will be destroyed locally within the image by any subsequent image processing, and any regions so modified will be identified by a comparative analysis program which will establish which image is the "original" or that no modifications have been made because no changes are detected.

However, the system is not foolproof as it cannot cope with the problem of the trusted insider within an organisation who keeps an unmarked image, alters it, and then adds the invisible watermark. Therefore it is important to be able to establish that the addition of the watermark can be guaranteed to occur at time of capture.

Dr Jian Zhao of the Fraunhofer Centre for Research in Computer Graphics writing in Byte: p 7 January 1997 distinguishes between the purpose of a digital signature as ensuring authenticity and integrity in documents, and watermarking as the identification of authors and authorised users notwithstanding processing and partial distortion through analogue to digital conversion, low pass filtering, resampling, lossy compression, cropping or rotation. He concludes that "none of the currently available watermarking systems will survive all imaging or signal processing operations. But like encryption, this technology will be useful as long as it makes tampering with or removing watermarks a time consuming and costly task."

From the above, it can be seen that watermarking techniques should be distinguished from encryption which involves file transformations to make the original image unrecognisable.

QUESTION 3.1

What would be the preferred practical measure?

The appropriate use of watermarking, digital signature and security products and techniques, coupled with adequate processes, can ensure that reliable evidence of the time of creation and integrity of the images is available.

Which products, techniques and processes are appropriate will vary according to the requirements of different types of user. IBM considers that users should be free to choose the most appropriate form of authentication and security to meet their business and legal needs.

It would not be appropriate for the law to mandate that any specific security or authentication techniques be applied to images as a precondition of admission as evidence. However some commentators, such as Roderick McCarvel (<http://www.seanet.com/rod/digiphot.html>) recommend that digital cameras intended specifically to gather evidence of eg, bad driving, accidents and roadside interviews by law enforcement agencies, should be required to include verification technology. IBM would endorse the optional inclusion by the manufacturers of such technology.

QUESTION 4

Under what circumstances and with what controls should modified or enhanced images be used as evidence?

Enhancement is the manipulation of the image to make some areas more distinct than in the original. If done carefully, this process does not introduce artefacts and may therefore be considered more reliable than modified images. Although excessive enhancement may introduce image artefacts which undermine the reliability of the data, it is usually possible to determine whether the image has been "over-enhanced".

Modified or manipulated images have had regions accidentally or deliberately altered. These alterations are irreversible and may be undetectable.

Compliance with system security best practice recommendations such as those contained in the British Standards Institution Code of Practice for Information Stored on Electronic Document Management

4 December 1997]

[Continued]

Systems (DISC PD 0008) on the legal admissibility of digital images, and in particular the procedures and the use of non erasable Write Once Read Many storage devices, ought to be a relevant consideration in the Courts' assessment of the probative value of modified or enhanced images. Failure to comply with such standards should not however be grounds for the inadmissibility of such evidence. Modified or enhanced images should be admissible in evidence under the same conditions as evidence of unmodified or unenhanced images. The Courts should decide on the authenticity of any such images on the basis of all relevant matters including audit trails, which can if necessary be supported by expert evidence in cases where authenticity is in issue. Extraneous factors such as time and space incongruities, and the motive, means and the veracity of witnesses will often be relevant. Courts are well versed in assessing such matters as the chain of custody, the presumption of regularity and the integrity of a system.

QUESTION 5

Do technologies which compress data or use error correction technology when transmitting it raise special problems?

Error correcting codes are very commonly employed in daily use in many of our ordinary activities, eg, telephone, fax, all computer systems, especially on hard disk drives, credit cards, bank transactions, etc. There is no evidence that error correction today has any effect on image validity.

Compression is a specialised technique, which if done inexpertly can result in inaccuracies. Results will vary according to the compression technique employed and the characteristics of the original image.

The purpose of compression is to reduce file size and therefore storage cost. There is a trade off between image detail and compressed file size. Compression comes in two major forms—lossy and lossless.

Lossy compression achieves its aim by deliberately losing some detail in the image. This detail may or may not be critical. Images which have been compressed using a lossy algorithm are easily detectable by computer programs, though not necessarily by human sight.

Lossless compression will deliver back the original image and therefore should be used for images which must be guaranteed recoverable from the compressed state. Lossless compressed images will usually be bigger than lossy compressed ones.

There is also an emerging class of compression technique—the regenerative technique based on fractals. Images which are compressed by these techniques may under some circumstances introduce artefacts when decompressed. This image technique must at present be regarded as less reliable for evidential purposes.

QUESTION 6

Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?

IBM recognises the importance of these issues of public policy but has no special competence to offer an opinion, other than to comment that most CCTV cameras in use today are connected to analogue recorders, so that care needs to be taken in ensuring that they are adequately maintained as worn tapes and dirty lenses often degrade image quality.

QUESTION 7

Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?

IBM considers that the placement and use of surveillance cameras should be subject to the same principles as those to be contained in the implementation of the EU Directive on Data Protection (Directive 95/46/EC) which is due to be implemented in the United Kingdom by 24 October 1998.

The Data Protection Act 1984 already provides certain safeguards in relation to some forms and uses of surveillance equipment, including regulating the release of information collected using such techniques. Although the mere capture of “personal information” (that is, information about identifiable living individuals) in the form of digital images is not covered by the Act, where those images are to be stored on computerised equipment and indexed in such a way as to allow the automatic location of information about a particular individual then the Act applies to regulate the collection, use, disclosure and transfer overseas of that information, unless otherwise provided for by the Directive.

An individual about whom the surveillance images are being processed will be able to ascertain the purposes for which the images are being used and request a copy of the information held. Until the Bill implementing the directive is published it is not possible to comment on any safeguards it will provide on the use and manipulation of surveillance images. In many respects Directive 95/46/EC is broader than the existing UK law and so it is likely that regulation in this area will increase rather than diminish.

4 December 1997][Continued

QUESTION 8

Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?

Law enforcement officers, the courts and the legal profession generally should be made aware of the technical possibilities and limitations presented by different digitisation products.

QUESTION 9

Is there the need for special measures to control the publication of modified images by the media?

IBM recognises the importance of the issue but has no special competence to comment on this matter of ethics and public policy.

Answers to Additional Questions Received on 27 November

QUESTION 1

Soon we can expect widespread access to equipment that can be used to modify images. What are the major implications of this for the courts? How easy is it to demonstrate in court that digital images represent what was first captured and have not been interfered with before presentation as evidence?

There should be no major implications for the Courts. Digital images are being admitted as evidence today without difficulty. The technology is a natural development from existing digital technologies with which the Courts are familiar, such as word processing and fax transmissions (which are binary digital images of text), and may present positive evidentiary opportunities for the identification of content owners and of unauthorised modifications in ways which are not available to traditional analogue technologies.

It may be helpful to distinguish different types of evidence useful to establish authenticity and the integrity of the chain of custody:

- (a) Procedural evidence to show that the image was captured with a correctly-working device and that the audit trail or chain of custody has been unbroken. This may include evidence to show the efficiency of security measures and working practices in preventing tampering. It may also include evidence of timed deposit with a trusted third party or digital notary.
- (b) Technological evidence to show, for example, that some watermark or digital signature has been placed in the image at its time of capture and is undamaged, or to show that the image has been protected within a tamper-proof system, such as an IBM Cryptolope, since its capture, or to show that the image was immediately written to a WORM disc and thus preserved intact.

QUESTION 2

Can you tell us something about the use of watermarking. It has been suggested to us that a "fragile watermark" or a "digital signature" are techniques which might be used to demonstrate to a court that a digital image is an accurate copy of the "original". How useful are these technologies for that purpose?

See answer to Question 3 above.

IBM researchers at The T.J. Watson Research Laboratory have developed such a fragile digital watermarking method which is resistant to attack, and which very clearly shows whether or not an image has been manipulated. Also, unlike some other digital watermarking schemes which only give a yes or no answer to the question of tampering, the IBM method shows exactly which portions of a falsified image have been changed. We also understand that Primary Image, Ltd. (<http://www.primaryimage.com>) make a surveillance system which uses watermarks as a means of making its images tamper-resistant, and that an image of this type has been used successfully in court.

QUESTION 3

Are you aware of other technologies which might be built into digital imaging systems which could be used to detect alterations to those images (whether intentional or unintentional) between the time they were recorded and the time they were produced before the court?

We are not aware of any other specific technologies currently available for this purpose. However, research into image processing and digital watermarking continues and the pace of change is so great that it is always unwise to limit one's vision to the currently existing methods.

4 December 1997][Continued

QUESTION 4

How do you see the relative merits of procedural measures, like audit trails, and technological measures such as watermarking and digital signatures? If you think such measures are needed when images are used as evidence, how should they be achieved eg legislation, rules of court, standards, codes of practice or something else?

Procedural and technical measures are complementary. For example a thorough audit trail needs to be kept of the processes that were used. Transaction logs need to be kept for non-repudiation purposes, and the time-stamps on these logs need to be secured. A whole structure of trust needs to be established and "rooted" in an ultimately trusted party to ensure that when a signed document is validated, the chain of trust from the signer through the certification authority and beyond needs to be verifiable.

Whilst both procedural and technical measures play a part in increasing the probative value of the evidence, it would be inappropriate to make either mandatory. The ideal would be to have available to the Court a watermarked, time-stamped, signed image that had been "wrapped" in an IBM Cryptolope or equivalent, and that had been stored immediately on a WORM disc, without any form of compression, or communication outside a closed secure system. A complete audit trail would be available, as also would the "photographer".

In practice the use of each of these measures increases cost. For example, most digital images are rather large files; storage costs can be reduced by compressing the files, but some methods of compression may cause artefacts to appear in the later decompressed image. If the law were to mandate that no image that had ever been compressed would be admissible as evidence, because of the danger posed by such artefacts, the burden of cost to companies and public bodies would be very great, and disproportionate to the evidentiary benefit.

QUESTION 5

It seems at least possible that any document or image may at some stage have been subject to electronic storage or Electronic Document Interchange (EDI) ie, storage/transmission. Do any measure you envisage as necessary to determine the evidential value of computer processed images or documents have to be put in place for all documents or images?

We do not believe that any technological or procedural measure is absolutely determinative as to the evidential value of a digital image or document. None of these measures is foolproof, and none can, or should, take away the role of the court as the finder of fact.

While it is true that these measures will tend to increase the evidential value of digital documents and images, the burden of cost makes it unrealistic to make the use of them mandatory for all documents and images, most of which will never be used as evidence, or which, if they are, may never be contested. Companies and public bodies may need to examine their use of digital material to determine which records are likely to be at risk and to make provision accordingly.

QUESTION 6

Do you agree that there may be an imbalance of access to resources between prosecutor and accused or plaintiff and defendant? Do you think that the increased use of technical measures such as the watermarking of originals would help redress any imbalance or would it simply create further difficulties?

IBM does not have any particular competence to comment on this issue.

QUESTION 7

In your opinion do the courts, the judges, barristers, solicitors, have the appropriate skills to contest the reliability of images? Is there a difference between the criminal and civil courts?

Whilst IBM does not wish to comment, personally I consider that the legal profession is increasingly knowledgeable, and is well suited to determine the issues presented by digital imagery. The level of expertise and experience is high and increasing as the legal relevance of these technologies increases.

4 December 1997]

[Continued]

QUESTION 8

Finally, and I realise this may be outside your strict remit, do you think video evidence, or computer processed documents, should ever be accepted as the sole evidence against a defendant if these measures are not in place? Should the jury in a criminal case be warned by the judge of the implications of the absence of such procedural or technical measures?

Personally I consider that there is no reason why video evidence or computer processed documents should be treated differently from evidence derived from other sources, even in cases where no corroborative evidence (or in the technical sense no parallel modalities) exist. Such evidence should be admitted but only be accepted as the sole evidence against a defendant if it can be shown to satisfy the appropriate criminal or civil burden of proof. The presence or absence of corroboration through procedural evidence or authentication and verification techniques will clearly affect the weight to be given to such evidence. Whether or not a jury should be warned by the judge in a criminal case of the implications of the absence of such measures should in my view be a discretionary matter for the judge to decide.

Examination of Witnesses

MR ROBERT MARCUS, Senior Counsel, IBM and MR SYD CHAPMAN, Research Scientist, called in and examined.

Chairman

260. Mr Marcus, welcome to the Committee. I understand that Mr Chapman is delayed by traffic, travelling problems, no doubt, but will be joining us later. As you know, our interest is really in the use of digital images as evidence. We are in the process of taking written and oral evidence and you have kindly submitted a very valuable piece of written evidence, and I thank you for that. I should explain to you that my colleagues have not all yet actually received it, but it will be made available to them. Bear with us therefore if we appear to ask a question to which you have already given an answer. There will be supplementary questions. May I ask you to say who you are for the record and ask whether you have any opening statement that you would like to make before we dive into questions.

(Mr Marcus) My Lord Chairman, thank you. My name is Robert Marcus and I am a solicitor employed by IBM Corporation. I work in the Hursley development laboratory near Winchester and I have done so for three years. I do not have any opening statement, my Lord Chairman.

261. Thank you, Mr Marcus. May I start then by asking you about the major implications of widespread access to equipment that can be used to modify images for the courts? How easy is it to demonstrate in court that digital images represent what was first captured or, indeed, how easy is it to challenge that perception?

(Mr Marcus) My Lord Chairman, I should like to refer, if I may, to the written answer that I made to the first supplementary question which has been submitted this morning. I believe that there should be no major implications for the courts. Digital images are being admitted as evidence today without the evidence being challenged. The technology is a natural development from existing digital technologies with which the courts are familiar such as word processing and fax transmissions, which are binary digital images of text, and may present positive evidentiary opportunities; in fact for the identification of content owners and of unauthorised modifications in ways which are not available to traditional analogue technologies.

262. Have you had any particular experience yourself of any challenge then?

(Mr Marcus) Personally, I have not.

263. The inference then is that from your perception there is no significant difference as far as the courts are concerned?

(Mr Marcus) There are very significant differences between analogue and digital technologies, but I do not believe that the differences are sufficiently important to justify their being treated differently as a matter of law, the law of evidence.

264. You would apply that to both criminal and commercial law?

(Mr Marcus) Yes, I would, my Lord Chairman. I would rely on the different burdens of proof to establish stronger tests of evidential value in the criminal context in the normal way.

Chairman] Fine, thank you.

Lord Ackner

265. Is not one of the problems from the point of view of the weight to be attached once the digital image has been admitted the issue as to whether it has been tampered with because in order to establish that it has not been tampered with it can be a difficult matter, can it not?

(Mr Marcus) Yes. It can be a difficult matter in analogue technologies as well. It is certainly conceivable that in certain situations it would be almost impossible to establish that a digital image had been tampered with. There are, however, a number of procedural and technological matters that can be put in front of a court which will go to the weight and which will assist one party or the other in establishing the integrity of the image presented or the opposite.

266. But if the defence was going to seek to establish an alibi that he was not where the digital image is alleged to have occurred, it would be very easy to establish, would it not, that such is the technique that somebody could have transposed his head on the image at which one is looking?

(Mr Marcus) It would be possible to transpose heads on images and the technology is available: very

4 December 1997]

MR ROBERT MARCUS AND MR SYD CHAPMAN

[Continued]

Lord Ackner *contd.*]

sophisticated technology both in two dimensions and in three dimensions, and relatively cheaply available technology, to do those things. However, in order to resist a challenge from the other side in an action the party relying on it would have to demonstrate that it had not been tampered with and then all the traditional skills and attributes of the courts would come into play; the presumption of regularity, the evidence as to the integrity of the system, evidence as to the chain of custody, and you could then assess whether the party who was claiming that the image had been manipulated had the means, the motive, the technical and financial resources to do it, and you exercise a judgment and say, "It is extremely unlikely that this or that image had been tampered with".

Lord Phillips of Ellesmere

267. In that case, my Lord Chairman, in the light of the supplementary answer, may I ask whether your first answer should be taken to mean that there is nothing new, there are no new problems that arise through the use of digital images that do not already arise in the use of analogue images?

(Mr Marcus) I would accept that. The difficulties are different, but I do not believe that they are sufficiently different to justify different treatments as a matter of law. May I explain, my Lord Chairman?

Chairman

268. Please do.

(Mr Marcus) There have been techniques for forging images in documents for many thousands of years. The techniques in the digital context are different, but conceptually they are not different¹; they can be detected in almost every case². There are instances of analogue technology forgeries which are undetectable just as there are instances of digital technology forgeries which are undetectable.

Lord Nathan

269. Mr Marcus, you have just answered the sort of question that I was wanting to pursue. Supposing that I was defending somebody, as I understand it, if evidence were contained in an ordinary photograph, to put it in plain English, my understanding—I have always understood this—is that if I approach an expert in the field he could advise me whether this had been tampered with or whether it was a genuine photograph or not whereas I am told that if I went to an expert, however eminent, in relation to a digital representation, an expert could not advise me in that way. If what I am saying is right, this is a very substantial difference. I think that you have answered that question already, but that is the point which is in my mind and which, I must say, we have had some evidence on.

(Mr Marcus) My Lord Chairman, I would like to elaborate on what you mean by tampering. There are various things that you can do with digital images.

You can compress it, you can enhance it, you can modify it, you can embed in it watermarks which are both visible and invisible, fragile and robust, so that if appropriate precautions are taken it is very easy to detect tampering and manipulation. If no precautions are taken, it may also be possible. It is only with considerable skill that a digital forger could avoid the forensic skills of a suitably qualified digital detective.

270. But are you saying then, would you maintain, that it is as easy to detect—assuming no precautionary measures of the watermarking type that you mentioned—a manipulation or change in the image in the digital context as it is in an ordinary photograph, to put it in plain English? It is?

(Mr Marcus) It may be.

Lord Brain

271. My Lord Chairman, I think that we are getting back to almost the original photograph. Can you tell us what you mean by a fragile watermark or a digital signature? How can we know that an original is an original? I will take that as the first question because I have two supplementaries on it.

(Mr Marcus) Sometimes we cannot know. There is an environment in which a digital image can be faked. However, if there was a complete correspondence between the data set, if every pixel in a digital image has the same value as another data set, then it is the same. However, if one image is overwritten on top of another the original has disappeared and the copy becomes the original.

272. What about watermarking? How is that embedded in the file, shall we say, so that you cannot eliminate it because, as you say, if one does something you can always take something out as well?

(Mr Marcus) Watermarks can be either visible or invisible, depending on the use to which you wish to put them. A visible watermark is embedded within the visually perceptible part of the image by, for example, altering the luminescence of selected pixels. Invisible watermarks are embedded within some visually imperceptible part of the image signal. Robust and fragile is the other distinction. Robust watermarks can withstand image manipulations and can still be retrieved intact. Different schemes will be robust against different types of manipulation depending on where in the signal the watermark has been placed. Fragile watermarks are retrievable after image manipulation, but they are demonstrably damaged by the manipulation, and these are good for demonstrating that an image has been tampered with.

273. So that what you are saying is that, suppose we have got an image of a face, head and shoulders, and the head has been changed but the shoulders have not, it might be possible to detect with a robust one that the watermark is still there, and with a fragile one, that part of the watermark is there and part of it is not, is that what you are really trying to say?

(Mr Marcus) If you take out a piece of the image and that is the piece of the image in a visible

¹in the sense that the underlying intention is to deceive through manipulation.

²But only if an "original" copy exists.

4 December 1997]

MR ROBERT MARCUS AND MR SYD CHAPMAN

[Continued]

Lord Brain *contd.*]

watermark which you can see, you do not actually destroy the watermark because there are changes in the pixel values distributed in a random way throughout the data set.

274. Fine. Now, going on, I think that one of the things that we are looking at is not necessarily what the system is now but what we feel that it should be in the future. If we go back again to photographic technology, the image is recorded in the centre and there is other information round the margins that are never seen when it is projected, but one can go back and look at the footage or the image number and things like that. Is it possible, using modern programming, to design a system so that the image on the camera is recorded in one part of the database and the time and the location or whatever, the other data that are relevant, can be stored in a parallel file, and then perhaps when the master file is downloaded you can also record in the parallel file that it is downloaded on such-and-such a date or some information like that? It is really trying to see how one can start the audit trail, then possibly be able to follow it electronically as with a photographic film you can follow it?

(*Mr Marcus*) A still image or a series of images on a video can be authenticated by the use of time stamping, whether it is actual time or location or some biometric or other electronic fingerprint which can be placed visibly or invisibly within the data stream. There is no reason why it should not—I think that there is good reason why it should—be kept in a separate part of the database or a separate database so that the audit trail can be examined separately. It can be made more secure by the use of cryptographic techniques and by the use of notarial techniques, by the use of trusted third parties, or, indeed, in the case of some audit systems which use third party notarial systems there is no requirement to trust a third party. It is a feature of the software that it automatically creates a hash or a digital signature of that stream of video images which, without the scope for dispute, identifies the source from which it came.

275. Then I have quite a small question, my Lord Chairman, first, the question of cost, is it expensive to do this, and then the cost of computer power. Running a separate file obviously does cost computer power. Is it expensive or relatively cheap?

(*Mr Marcus*) All these technologies running in parallel for certain purposes would, I think, be disproportionately expensive. I think that the questions of costs need to be assessed in relation to the purpose for which evidence is derived. Certainly there are some commentators who believe that equipment specially designed for capturing criminal evidence such as speeding roadside interviews should have embedded verification technology. Our view is that that would be an optional feature which manufacturers of these pieces of equipment should be able to provide.

276. But not necessarily specify as essential?

(*Mr Marcus*) Correct, yes.

Lord Tombs

277. Mr Marcus, are you aware of any other technologies which might be built into digital imaging systems which could be used to detect alterations to those images, intentional or unintentional, between the time that they were recorded and the time they were produced before the court, and I really mean a way that cannot be overridden, of course?

(*Mr Marcus*) My Lord Chairman, yes, I am. They are essentially some of the technologies that I have mentioned already, watermarking in its various forms, and there are Cryptolopes which are an IBM proprietary product. Cryptolopes wrap content in a cryptographic signal which can only be decoded with appropriate software held by the other party. Then there are digital signature technologies.

278. That well describes the method of originally marking the first copy. What I am really looking for is a log of operations that have taken place subsequently, the use of enhancement techniques, straight copying, comparing, deliberate intervention. Is that a practical proposition?

(*Mr Marcus*) All of those things can be done.

279. In a secure way or in an ostensibly secure way?

(*Mr Marcus*) Some of those technologies reduce the security, but in some contexts it is a trade off that is worth making. For instance, compression is useful because it reduces the cost of storage.

280. It does seem to me that the evidential quality of a digital image would be greatly improved if one had first of all the original image stored in a secure way, perhaps on a WORM disk or something, and sealed; and then subsequent attempts to process the thing, intentionally, as I say, or unintentionally, were locked so that the image being presented would say, "Since the original the following operations have taken place".

(*Mr Marcus*) That is relatively easy to achieve with comparative programmes comparing the original with what is subsequently presented.³

281. That I regard as the ultimate. I was wondering whether the image being presented could also carry its history?

(*Mr Marcus*) There is no reason why it should not, as far as I am aware, my Lord Chairman.

282. In a secure way?

(*Mr Marcus*) Yes.

(*Mr Syd Chapman here joined the meeting*)

Chairman] Mr Chapman, on behalf of the Committee may I welcome you to the witness table. We are very pleased to see you here. I will leave it to Mr Marcus to invite you to respond to any of our questions as and when he feels it appropriate.

Lord Brain] My Lord Chairman, I wonder whether Mr Marcus has got anything from what we have already been discussing that he feels Mr Chapman might wish to comment on?

³Assuming an audit trail exists.

4 December 1997]

MR ROBERT MARCUS AND MR SYD CHAPMAN

[Continued

Chairman

283. Mr Marcus?

(Mr Marcus) My Lord Chairman, Mr Chapman is better qualified than I am to discuss the technologies and the applications of watermarking.

Lord Brain] Perhaps we might come back to that, my Lord Chairman.

Chairman] When we come to look at the evidence, if there is anything there that Mr Chapman might feel would be helpful to us to add to what you have already said, Mr Marcus, then there is an opportunity to let us have that. May we move on now to the next question. Lady Hogg?

Baroness Hogg

284. Mr Marcus, earlier—and I am summarising slightly—in regard to forgeries and the law you described two responses, one of which was procedural and the other of which was technological. As we go through phases in technological development, however, we find ourselves in periods where the technological responses or defences may lag behind or may catch up with the initial development that permits more sophisticated forgeries. Where we are now would you place greater weight on procedural process defences or technological defences to ensure that the courts could rely on digital evidence?

(Mr Marcus) As you know, my Lord Chairman, it is a feature of the technology that it is growing and developing very rapidly and that power is increasing and cost is reducing. Innovation is extremely rapid, and therefore what the position is today may be radically different tomorrow. Also I would say, in direct response to the question, that I think that the two types of evidence are complementary. They need to be seen together. In fact, they are probably meaningless if they are divorced from each other. I therefore would not put greater weight on one as opposed to the other.

285. Would you like to elaborate on that a bit, Mr Marcus? Of course you have to talk about the process in the context of the technological devices you built in to protect the process or to enhance the process, but perhaps you would say a little more about your model for establishing the validity of a piece of digital evidence?

(Mr Marcus) The idea would be for a piece of digital evidence to have embedded in it evidence of its own originality at the time that it was created. It would then be transmitted and processed in a system that was secure from people or other processes that may inadvertently or deliberately wish to manipulate it, and the system itself would incorporate all the best technical defences and would be operated by people who were trustworthy, within an institutional structure which was secure; and then you would have, I would suggest irrefutable evidence of originality and lack of manipulation.

286. But would you at this present moment be inclined to place greater weight on ensuring in cross-examination of evidence or whatever that you were comfortable with the people who were in charge of the handling, that they were, as you described, trustworthy, or on in-built technological defences?

(Mr Marcus) My Lord Chairman, I think that it would very much depend on the case.

287. Go on.

(Mr Marcus) In a case where the people and the technology in the context showed that the opportunity for sophisticated technical forgery was low I would look to the procedures and veracity and the trustworthiness of the people in a traditional way. When it was, if you like, a high tech context where the opportunity and the means and the motive were available to one or other of the parties to do this, I would look very much more closely at the technology.

288. Let us take this one a bit further, my Lord Chairman. If one is looking at whether there is a need for some kind of set of regulations to deal with digital evidence, then you are talking about placing weight on technological defences or requiring those who produce the evidence to fulfil certain criteria as to the kind of people and the kind of oversight of the kind of people and licensing of the kind of people who are involved in this process, and that is why I am trying to push you a bit on this. Look at it from our point of view and say, if you are trying to give some comfort or trying to come to a point where we can subscribe to your view that there is really no problem here that is any different, are there process type regulatory systems that we should be looking at to reinforce this?

(Mr Marcus) Yes, certainly, my Lord Chairman. There is best practice within the computer security arena which will describe good computer systems from this perspective. They use all the traditional means such as pass words and ID and keystroke recorders and back up copies, WORM disks and separate time stamping verification streams within parallel databases. All of those things exist and they are available, and in the correct context they represent best practice in a particular situation. The British Standards Institution has promoted best practice for the storage of electronic data and the purpose of that, as I understand it, is to enhance the evidential value of the data presented to a court by a party who can demonstrate that they have adopted best practice, and one measure of best practice is conformity to a standard. I would not, however, exclude evidence which had not been obtained on systems complying with such standards as a matter of the law of evidence.

289. So what would you exclude?

(Mr Marcus) I would exclude nothing. I would leave it to the court to form its own judgment on the weight of the evidence before it.

Chairman

290. In an earlier comment, Mr Marcus, you referred to a trusted third party as one form of giving confidence to the courts that material which is presented has been properly looked after. I wondered whether you would like to expand on your thinking about the need for a trusted third party, whether you feel that it is just another desirable element of giving confidence to the material presented to the courts or whether you see it perhaps—and bear in mind that we are talking of digital images—as an area where

4 December 1997]

MR ROBERT MARCUS AND MR SYD CHAPMAN

[Continued]

Chairman *contd.*]

that arrangement, a trusted third party arrangement, would be desirable? Mr Chapman?

(Mr Chapman) My Lord Chairman, I am sorry I have not heard the previous context, but the background to the trusted third parties has really evolved from the requirements of encryption techniques for holding keys, that they can be extended to techniques whereby a document which is valid can have some kind of hash or encryption or key associated with it which is held by the third party and that third party then will issue a private key back to whoever is trying to look at the document. The requirement there obviously is, how do you actually ensure that the third party is truly trustworthy.

291. And so on ad infinitum?

(Mr Chapman) Technology cannot solve that problem, my Lord Chairman.

Lord Phillips of Ellesmere

292. We are not in general in this context dealing with petty crime, I think; we are dealing rather with crime which might be regarded as a major enterprise almost. The people involved are not short of resources. They have access to all of those technologies that you have been describing. What is to prevent them fabricating so-called evidence to the highest standard, even including the audit trails that go with it?

(Mr Chapman) My Lord Chairman, if and only if the image has information embedded in it at the time of capture and that information has been encrypted in a way which allows you to be certain that it cannot be decrypted by any mechanical process without the key, then you have a sound starting point. If at any time you have an image which has passed out of your control without any kind of encryption, time stamping, signature or whatever in it, then you have no control at all, but with strong encryption in the image itself at the time of capture, then you have a starting point where you can use any kind of technology—third party keys or otherwise—to ensure that the original image is the one that you claim to be the original one. At that point if you have a sound starting point, then you can apply technology to detect changes, and it would be very difficult given the amount and the speed of computers today to break some of the codes in a reasonable time. I think that in all of these processes the only thing that you can do is make it very difficult, and if you can make it difficult enough, such as that the process takes too long, then you are at least achieving part of your aim. However, I do not think that technology will ever make anything 100 per cent secure.

293. So we look forward to an escalation of the problem?

(Mr Chapman) The problem will always be there, yes.

Lord Kirkwood

294. If I may just go back to the third party problem, the third party does not have to know the contents?

(Mr Chapman) No, does not have to—does not even have to have the document.

295. I see, nor the document. If the third party were, for instance, some government office or some statutory body which has nothing to do with the organisation, all that they would have to do is to record the times that that document was interfered with. That might be a possible better solution. One can always imagine situations where there are crooked people in all places, but if one had something at arm's length it would be better. As I say, it really has nothing to do with knowing what the document is; it is just recording the times that that document was looked at?

(Mr Chapman) The only thing that they can do is to record—if they do not have access to the document—new versions of the document. They cannot tell what has happened to it. They can merely recognise that a new version has arrived. Then you can track through the version and do whatever technological things you need to do to determine what has happened to the document in the steps from when it arrives in the custody of the trusted third party, but the trusted third party can do nothing actually to do anything with the document itself.

Lord Kirkwood] But it is quite important to know the occasions on which that is examined? That would be another little piece of evidence?

Baroness Hogg] Yes.

Lord Kirkwood

296. And they would have to justify or say what was done on that occasion? If it was not manipulated, they would be asked the question, what did they want it for?

(Mr Chapman) The difficulty is that the trusted third party as it stands today is not in any way in control of the document. If it is an image which I hold, I will keep the image and it is up to me whether I send you—because you are my third party—information as to what I have done with the image. Now, if I want that image to have a very clean audit trail, then I will send you information every time that I do anything. If I want to break the audit trail, then it is within my power not to send you any information when I make a change.

297. Putting you under an obligation to say why you did not do that?

(Mr Chapman) Yes.

Lord Brain

298. My Lord Chairman, I think that there is one thing that we may have missed in this last bit of discussion, and perhaps I should have picked it up earlier. Should we not have what might be called a master copy, possibly WORM, which is stored secure and, as is often used in interviews, what might be called a working copy which can be circulated, looked at, used, and then if evidence is later presented the secure master copy which may have been suitably filed with a third party or whatever can be withdrawn, a second working copy made from it—two working copies?

4 December 1997]

MR ROBERT MARCUS AND MR SYD CHAPMAN

[Continued]

Lord Brain *contd.*]

(*Mr Chapman*) If you can do that under guaranteed conditions, then you would have an original, which is what you are trying to work from, yes.

Bishop of Leicester

299. My Lord Chairman, I would just like to follow up the answer to the previous question, the technical matter that you have a third party who is a key holder and that third party has to be contacted before the image can be worked on; and then you said, yes, but you could continue to work on this image without actually telling the key holder. That is if there was a standard password, but would it not be possible to have a password that actually changes every time the image is manipulated so that one would have to keep going back to the key holder to get, in a sense, the updated key or the updated password?

(*Mr Chapman*) My Lord Chairman, I think that that may be my fault, creating some confusion there. Third parties may or may not hold documents. They may simply hold the key, or you may encode the document and give the whole document to the third party.

Baroness Hogg

300. On the master copy?

(*Mr Chapman*) On the master copy, yes, and then you would have to request it back to do something to it, but many people in industry do not want to do that. They do not want to give the document away, but what they want to do is to maintain an audit trail, and in that case they will not give you the document; they will give you a key signature for the document. The key signature is a piece of code which will enable you to define the state of the document. It is an indication of what condition the document or the image was in at a particular time. If I change the document the key generated will change so that the key that you have no longer matches the key I generate. In that case I know that the document has changed, but nothing else. In the other case I would encode the document in some way and send you the whole document, and then you know when I request it back, so you would have an audit trail, which is different.

Lord Phillips of Ellesmere

301. My Lord Chairman, I am a little unclear, and I speak from a basis of not great knowledge from the legal point of view, whether we are talking here mainly about evidence that is to be used on the prosecution side of the case or on the defence side of the case. Should we be requiring defence evidence to be subject to the same sort of conditions if it is to be taken seriously?

(*Mr Marcus*) My Lord Chairman, I would not want to make that distinction at that level because the techniques and the technologies could be available to either party.

Chairman] Right, I think we should move on now. Lord Brain?

Lord Brain

302. My Lord Chairman, I think that we have circled question number five fairly well. I would just press about the final part, that is, to what degree would you envisage the necessity of putting all these things, and I got a reply earlier that, yes, all can be done, but you have got to have to do what I might call risk assessment and decide whether you have to put in a huge file to follow what has happened because there is a chance once in a thousand years that you are going to come back to this? Where is the balance? I do not think that we need a very long answer, my Lord Chairman.

(*Mr Marcus*) My Lord Chairman, I would put it in the court of the user, the person who will in the future or may in the future wish to rely on the evidence that they are presenting. If they know that there is likely to be contention and it is likely to be subject to sophisticated manipulation, they should decide for themselves what technology and what procedures are appropriate in order to enhance their chances of being able to establish the evidentiary value of the digital images.

303. So that if it is going to cost you £100,000 you may take a different line from if it is going to cost you £100?

(*Mr Marcus*) Correct.

Lord Ackner

304. I expect that you envisage, do you not, that in a criminal case certainly there will be an imbalance between the prosecution and the defence certainly to start with as to the resources that are available to apply to the integrity of the digital images?

(*Mr Marcus*) My Lord Chairman, it is certainly possible.

305. In that situation do you think that the imbalance can be addressed by the use of technical measures such as you discussed?

(*Mr Marcus*) If they show that the prosecution evidence has been tampered with, then if it has been tampered with inexpertly or if there is any breach in the chain of custody or actual evidence that the manipulation has been done poorly, then that will rebound against the prosecution evidence in that case.

306. That is one concern. That goes, as you say, to the weight, not to the admissibility?

(*Mr Marcus*) I do not believe personally that there should be differential rules about admissibility based on the technology with which the evidence is generated and presented.

Chairman] Are there any other points on that? Lord Ackner, do you want to go on?

Lord Ackner

307. I do not quite know what your court experience is, Mr Marcus, but have you reached any conclusions as to whether there are the appropriate skills and knowledge amongst either the court or the advocates in order to contest the reliability of images?

4 December 1997]

MR ROBERT MARCUS AND MR SYD CHAPMAN

[Continued]

Lord Ackner *contd.*]

(*Mr Marcus*) With respect, my Lord Chairman, they are not ignorant; they are very skilful in my experience. My experience of forensic digital evidence is very limited, my Lord Chairman. However, I have much exposure to courts and to the judiciary in various forms in this country, and I have always been very impressed by the technical skills and knowledge that is displayed. They are, of course, supported by expert witnesses who can assist them.

308. Is your experience limited to the civil courts or does it encompass the criminal courts as well?

(*Mr Marcus*) My experience is essentially limited to the civil courts. Mr Chapman has had some personal experience of the criminal courts.

309. When you say the civil courts, is there a further specialisation within that, namely, commercial courts and the official referee?

(*Mr Marcus*) My Lord Chairman, for the last ten years or so I have been in house counsel for IBM and one of my tasks has been to reduce litigation to the minimum amount, so it is only my previous experience that led me into daily contact with the Commercial Court.

310. I believe that you have had some experience on the criminal side, Mr Chapman?

(*Mr Chapman*) My Lord Chairman, I have some experience on the processes whereby digital images can be enhanced to produce evidence which was later used: I was one of the people who worked on the James Bulger video. We were asked whether we could enhance the images in order to—well, in my case I was asked whether I could enhance images in order for the police to be able to contact people because they could not recognise who the people were in the image, so my experience was to take some images which were very poor quality video and to improve the quality of the image such that the people in them could be called upon to come forward themselves. It was not a case of, “Provide me with an image so that I can go and find someone”; it was, “Provide me with an image from which we can ask people to come forward to verify where they were at that particular time”. The difficult part of all of the image processing techniques is how far you go before you introduce artefacts into the image which can create a false impression.

311. What do you mean by artefacts?

(*Mr Chapman*) You can distort an image either deliberately or accidentally. Deliberate distortion can put people in different places, and I actually have some images here which you may want to look at, my Lord Chairman. However, if you do image processing such that you over-process, you can produce artefacts in the image which may change subtly the image, the outlines, the colour of someone's clothing, those kinds of things, and that may not be deliberate, but you can do it if you are not careful, and that may or may not make the evidence not useful to you.

312. In the Bulger case was your activity merely to assist the police in their inquiries or were you

involved in the production of material that was used actually in evidence?

(*Mr Chapman*) I was asked to assist the police in cleaning some images and creating better images for their use, whatever use they were making of them afterwards. I was not involved in the case itself.

Baroness Hogg

313. My Lord Chairman, may I just follow that line of questioning and ask if either of you have knowledge or experience of the relative level of skill and expertise at the level of magistrates courts

... commercial litigation ... criminal cases ... widespread use in quite small cases. Do either of you have knowledge of those?

(*Mr Marcus*) My Lord Chairman, I have no personal experience, although I understand that a successful prosecution has been brought for assault based on digital imagery from a company called Primary Image using 2nd Eye software which was used successfully to prosecute somebody in an airport car park.

314. No, I am talking at a much lower level, the infringement of traffic regulations based on closed circuit television, say?

(*Mr Marcus*) I have very little personal experience, but my impression is that such evidence is usually accepted without challenge.

Baroness Hogg] Yes, all right, I will leave it there, my Lord Chairman.

Chairman

315. The clock is beginning to beat us, Mr Marcus and Mr Chapman. Are there any other points that you would like to make before we draw the session to a close? Mr Marcus?

(*Mr Marcus*) My Lord Chairman, no, thank you.

316. Mr Chapman?

(*Mr Chapman*) My Lord Chairman, one of the things that I wanted to do just very quickly, if I may, is to show the Committee some images, if that is permissible, in regard to what happens when you do things to images. Perhaps that would be useful, my Lord Chairman.

(*Mr Chapman handed round a number of photographs on which a brief discussion took place off the record*)

317. Thank you, Mr Chapman. May I thank you both very much, Mr Marcus and Mr Chapman, for coming to give evidence to us. You have been very helpful. Thank you also for the written information you have submitted, which we will be studying with care.

(*Mr Marcus*) My Lord Chairman, thank you.

(*Mr Chapman*) Thank you, my Lord Chairman.

4 December 1997]

[Continued]

Written Memorandum by Abbey National plc

IMAGING TECHNOLOGY AT ABBEY NATIONAL

Abbey National has a number of business systems that make use of image technology. The main drivers for these image based applications are operational efficiency and customer service. The ability to maintain a digital archive and to destroy paper originals has not been a powerful factor in these applications although this would be a future advantage once legal considerations are resolved. At present the aim is to remove paper from the processing of documents rather than to remove the paper altogether and no documents that would normally be archived are destroyed. There is a policy governing the retention of all documents and this policy is applied whether or not the document has been digitised.

There are currently four business areas with image systems, in these areas all incoming documents are scanned upon arrival. The scanned image is viewed by an operator for readability and at that point it is indexed and stored, usually on an optical storage device known as a WORM drive. WORM stands for "Write Once Read Many" and once the image has been digitally stored in this format it cannot be changed. If annotations are required these can be attached in the form of "overlays" but the original cannot be altered. This image is held in a central store and can be viewed by any other user on the system. Customer service is enhanced because documents can be retrieved immediately when dealing with telephone queries, for example.

At the same time as the document is indexed it is attached to a Workflow system and delivered electronically to the appropriate clerks for processing. This is where the greatest benefit to the business is achieved. By eliminating paper, processing is more efficient, documents and files are never lost or misplaced and work throughput can be managed more precisely by supervising staff. External consultants have estimated that up to 20 per cent of processing costs can be saved through the use of Workflow. Earlier pilot systems that evaluated image systems without workflow could not achieve sufficient savings or benefits to justify full adoption of the technology.

It is always necessary to authenticate documents before they are processed. In normal processing the risks of loss, damage or alteration of paper documents exists throughout the whole process, which could involve several people over a protracted period of time. When using digitised images, however, the risks are reduced by limiting exposure to the single point of capture. It is possible, then, to concentrate on secure management of the scanning stage. At Abbey National we will be guided by the BSI PD0008 Code of Practice and we have already tested our procedures against these draft standards.

During subsequent processing of digitised documents, the major risk is from substitution or deletion as the ability to edit images is not available to users. This risk can be controlled by means of audit trails which will record all accesses, including deletions and substitution.

Digital signatures and Watermark technologies were sought from suppliers during a strategic review two years ago. Such technologies were not commercially available at that time. We believe that the use of watermarks and digital signatures will provide additional security where documents and transactions are passed electronically between two or more organisations or individuals. Abbey National would, in these circumstances, like to see these methods accepted as valid, but not mandatory for the purposes of authentication and non-repudiation.

Abbey National has no experience of using digitised images as evidence in any court of law and will not be content to rely on them until their legal status has been confirmed.

Examination of Witnesses

MR PETER LAZARD, Head of Technology, Strategy and Research, MR DILEEP DAMLE, Senior Consultant for Technology, Strategy and Research, and MR MICHAEL URMSON, Senior Analyst for Technology Services Group, Abbey National plc, called in and examined.

Chairman

318. Mr Lazard, may I thank you and your colleagues very much for coming to appear before us today. Would you be kind enough for the record to introduce yourself and your colleagues?

(*Mr Lazard*) My Lord Chairman, I am just recovering from a cold so I hope that I can project my voice. My name is Peter Lazard and I am Head of Technology, Strategy and Research at Abbey National. My two colleagues are Dileep Damle, who works with me in strategy, and Michael Urmson, who is responsible for our software infrastructure supporting image systems.

319. Would you like to make an opening statement, Mr Lazard?

(*Mr Lazard*) My Lord Chairman, I have produced a short paper which I hope fairly well sets out the position with images at Abbey National. There is nothing that I would like to add to that, but I can summarise it if that would be helpful to the Committee, my Lord Chairman.

320. Perhaps we could start then on the questions. You at Abbey National have found it necessary to use imaging technology to meet your document handling needs. I think that it would be helpful to get an understanding as to why you have adopted that approach and whether there are problems that you

4 December 1997]

MR PETER LAZARD, MR DILEEP DAMLE
AND MR MICHAEL URMSON

[Continued]

Chairman *contd.*]

foresee in the future, bearing in mind the speed at which technology changes and the fact that new technology means that old technology quickly becomes, or can become, obsolete and cause handling or storage difficulties. Could you expand on that area a bit just to give us a feel for your experience?

(*Mr Lazard*) My Lord Chairman, we looked at digitally image based systems for many years. Originally we looked at them from the point of view of archiving, but we realised that that was not going to be cost effective, and it still would not be cost effective in our opinion, and that the only main reason for us to digitise images is to facilitate improvement in our process efficiency. By digitising documents we can take the paper out of the process. It is not really our prime intention to take paper out altogether in the sense of throwing it away, but it is more important for us to be able to take an image, digitise it and then process it in that form. The Workflow, which is the technology that is very closely associated with image technology, is the main benefit that we get out of imaging documents.

321. So in fact it is for commercial operational reasons within the company rather than for archiving, so do I understand that your policy is still to retain original documents in the paper form or whatever form they arrive in?

(*Mr Lazard*) My Lord Chairman, we have a document retention policy which applies to all the different types of document and we apply that regardless whether the document has been imaged or not. Technology has not changed the way that we retain documents, but if there are documents that we would not normally retain after that process, then we can clearly get them out of the way earlier in the process.

322. And just so that we are quite clear as to why you have resisted archiving in an electronic format, what were the arguments there?

(*Mr Lazard*) My Lord Chairman, I suppose that there is this fear that the documents would not be viewed favourably in court, and that is probably the main reason: it is perhaps just a fear. Everybody would say, well, that has not been tested in court, we don't want to make that move.

323. So this is a very firm belt and braces approach?

(*Mr Lazard*) Absolutely, my Lord Chairman.

324. What you know is what you are prepared to live with and you are not prepared to go out on a limb?

(*Mr Lazard*) Not the first, anyway!

Baroness Hogg

325. Mr Lazard, you said a moment ago that you will not keep documents that you would not otherwise keep, but as you become more comfortable with the system presumably you are hoping to move that boundary and keep less and less?

(*Mr Lazard*) Yes, my Lord Chairman, it would be our wish in the future to keep as little paper as possible. It is expensive to store obviously, and it is

difficult to retrieve, so we would like to be able to do that.

326. My Lord Chairman, that leads me on to the next question, which is the comparison of original and digital copy and how you can handle that both on a verification basis and a process basis?

(*Mr Lazard*) We capture an image, my Lord Chairman, and if I can talk through the procedure that might be helpful. An incoming document will be scanned at a central point. An operator will look at that scanned image in order to make sure that it is readable, legible, and that it is not upside down or whatever. If it is unreadable, then they will rescan it. Once it is acceptable and useable they will commit that copy then to a WORM disk.

327. You say acceptable?

(*Mr Lazard*) Acceptable in the sense that it can be read.

328. I do not want to push you towards the word perfect, but acceptable implies a slight edge to it there?

(*Mr Lazard*) Acceptable in the sense that people who will need to process from that document will be able to get the information that they need clearly and unambiguously.

329. And correctly, is what I am pushing for?

(*Mr Lazard*) Yes.

Lord Nathan

330. I appreciate that you are very cautious with regard to the position concerning litigation, but so far as the civil proceedings in which your distinguished company finds itself involved from time to time go, do you find that in discovery there is a tendency now to exchange documents by digital images on disk rather than the actual original paper? If so, I have some further questions to ask.

(*Mr Lazard*) No, is the answer, my Lord Chairman.

331. You are always dealing with the original paper in your discovery of documents?

(*Mr Lazard*) Yes, my Lord Chairman, at the moment, but it is an area where electronic transfer, the handing over of disks, may come into play.

332. But in your experience it has not yet?

(*Mr Lazard*) Not in my experience.

(*Mr Damle*) There is only one such initiative in the banking industry that I am aware of at this point in time. Within the banking circles in the process of clearing and settling cheques there is an initiative to exchange images of the cheques between banks in order to provide evidence of cheques that are in dispute. However, my Lord Chairman, this is still to come; it is by no means agreed at this point.

Lord Brain] You used the words, original image, but a photocopy is not the original image. Do you send originals to exchange or do you send photocopies? Do you fax them or do you use the postal system? Suppose that you have got an image on your computer, can you perhaps not use that to send directly off as a fax rather than use the original? If it is difficult to answer now, perhaps you would like

4 December 1997]

MR PETER LAZARD, MR DILEEP DAMLE
AND MR MICHAEL URMSON

[Continued]

Lord Nathan *contd.*]

to write to us. It might be better to have firm evidence rather than an off the cuff reply.⁴

Chairman

333. Mr Lazard, would you like to handle replying to the question in that way?

(Mr Lazard) Yes, my Lord Chairman, I think that we can.

Chairman] Thank you.

Lord Brain

334. My Lord Chairman, if I may just go back to audit trails, with Abbey National as a building society, now a bank, auditors must play a large part in the management or supervision of your business. What audit trails does Abbey National maintain in respect of each image and how useful would these audit trails be in proving the connection between the image and the original document and that changes had not been made? If any sort of thing has happened in the past, that a cheque has been written for £100 and someone has managed to add a thousand so that it is £100,000, how can this be checked and cross checked?

(Mr Lazard) My Lord Chairman, the original captured image cannot be accessed. It cannot be altered subsequent to its being stored, particularly on the WORM disk. Any annotation or work that is done on the document is done in the form of overlays to that original document, that original image, and the audit trail will identify where these overlays have been created, but it is still not possible to change the original.

335. So that, to go back to what I was talking about in the course of the earlier evidence, you have a WORM/original master and then you work subsequently and you may retain a back up copy on the working copy, would that be correct?

(Mr Lazard) Well, you use the WORM copy as your working copy, the same image, if you like, the one that is actually distributed to people.

336. The WORM stays there?

(Mr Lazard) It stays on the disk, yes.

337. But you will be producing another document image off your WORM for some other purpose, and I am not arguing about what the other purpose is, but that will nevertheless be retained somewhere in memory?

(Mr Lazard) It will be retained temporarily.

⁴To date, we have not transmitted a document that was stored in the system as an image to other organisations by electronic means. There is a common practice of converting a word processed document directly to an electronic facsimile and transmitting that. This is done as an alternative to printing the document on a piece of paper and then using a fax machine to send it. The facsimile form of the document sent would then be stored on a non-erasable medium for future reference. In our view, this practice cannot be construed as sending an electronic image of a piece of paper because the piece of paper was not created in the first instance. If the stored image had to be sent again, then a piece of paper would first be printed and a fax machine would be used.

338. Only temporarily, so once you have used it and done the transaction, you wipe it?

(Mr Lazard) Yes.

339. I think that covers that then, my Lord Chairman. We were talking earlier also about watermarks, methods of tracing the originality. If I can just go back to the photographic paper and things like that you could buy a watermark paper for copying purposes and things like that. What do you use? Do you find it necessary? Can you tell us your views on watermarking techniques and the need, if required, to demonstrate to a court that a digital image is an accurate copy of the original? I think you may reply to that, well, we use the WORM to keep the original so we do not need it, but let us hear what you say now.

(Mr Lazard) Well, yes, we might say that, but we have recently looked at the market of image systems providers and one of the criteria we were looking at in respect of potential suppliers was the ability to support watermarking and other security devices, not that they necessarily all could at the time that we were looking, but their ability to introduce those features later was something that was important to us. That having been said, whether watermarking or using any other device internally would be the ultimate defence for us is doubtful. I think that we would prefer to rely on procedures rather than technology, I suppose for the simple reason that you might watermark an image that you have captured yourself, but you cannot then prove that that is an image of the original paper. The paper may have been tampered with. I think that it is better to take your defences back to that original paper source rather than to believe in a defence mechanism that starts off halfway through the process.

340. So, just to go back to my cheque situation, what you are really saying is that, suppose the client who wrote the cheque for £100 has his account debited with £100,000, you would go back to the cheque and use a paper forensic scientist to say that that cheque has been tampered with or has not been tampered with rather than relying in any way on a digital image?

(Mr Lazard) Yes, at the moment, my Lord Chairman.

Lord Ackner

341. Have you yourself or your company got any experience of using your document images as evidence in either civil proceedings or criminal litigation?

(Mr Lazard) No, my Lord Chairman.

342. None at all?

(Mr Lazard) No.

343. Have you any anecdotal material of the experience of others in your field?

(Mr Lazard) Not of others, but internally we believe that we would be okay, so to speak, if we did use those images.

344. Nobody has tested it yet?

(Mr Lazard) No, nobody has tested it yet—and nobody wants to.

4 December 1997]

MR PETER LAZARD, MR DILEEP DAMLE
AND MR MICHAEL URMSON

[Continued]

Baroness Hogg

345. My Lord Chairman, may I just push that a little further, because, as Lord Brain said earlier, we do have to be careful what we mean here. On the cheque example, there are an enormous number of transactions of that size which have no physical body at all, they are done through an ATM. Have you had no legal cases challenging what has appeared on accounts drawn out of ATMs? Surely that must have used digital evidence somewhere down the line?

(*Mr Lazard*) I would not like to speak for that, my Lord Chairman, but I will take a look at it if you would like.

346. We are not in a world where everything is done by paper cheques any more. By definition I cannot believe that there have not been any legal cases?

(*Mr Lazard*) That is one reason why we would like to see images treated in much the same way as other computer based evidence and not necessarily given so much attention as being more vulnerable than any other digital evidence.

347. So you are making a distinction between computer based evidence and images?

(*Mr Lazard*) I think that it sounds as though everybody else is.

348. I am sorry, I am really trying to be clear. Therefore, when you are saying that you do not know of cases and so forth, what you mean is digital representations of physical objects as opposed to digitally generated or handled information?

(*Mr Lazard*) I am sorry, I have lost the distinction.

349. Perhaps you would like to make the distinction for me then between computer based evidence and digital images?

(*Mr Lazard*) I suppose that it is similar to what you were saying, that digitised image is a representation of a piece of paper or a document whereas in regard to what I would call computer based data it would not be an image on paper, it would just be the data itself, so that it is not an image representation.

350. You are talking of photographic evidence as opposed to digital evidence?

(*Mr Lazard*) Yes, my Lord Chairman.

Lord Nathan

351. My Lord Chairman, may I just explore that a little further. One of the great attractions, if I may put it that way, of the computer systems, to use a neutral term, is that if you have got scanned documents in a case you can have screens such that all members of the jury, for instance, can see exactly the same image which is presented as the judge and the counsel and so forth so that the image that they see on the screen is derived from a computer, it is what I would call digitised image, because it has been a scanned document, but people are not seeing, as it were, a television image of a piece of paper; they are seeing on screen what a computer has produced, and that is a digitised one, as I understand it, because it has been scanned perhaps from the original. Now, do you think that that is a safe way of working, and this touches on Lady Hogg's point as to where is this distinction between the computer aspect and the digitised aspect of the thing as you are putting it?

(*Mr Lazard*) My point is, should there be a distinction?

352. Yes, but how would you see the sort of instance that I have given? Would you look upon that favourably, that that is a convenient way of doing it? Undoubtedly it is convenient, but the question is whether the evidence is true and how it is to be tested. That is the problem—or perhaps you do not think that it is a problem at all?

(*Mr Damle*) My Lord Chairman, I think that there is not really a distinction between analogue and digital any longer. If you look at an analogue photocopier until quite recently you could make a photocopy, using an analogue process of creating a photographic image

which is then printed but most of those machines are now being replaced by digital photocopiers which scan the piece of paper first and they also perform enhancement techniques to improve the appearance and the readability of the piece of paper and so on. The fact of life today is that you can take an analogue image, convert it to digital, process and manipulate it and reconvert it back to analogue so that it looks like an analogue image. Now this is where I believe that the distinction is now lost because you now think that it is a TV analogue picture coming at you, but it never was.

353. Yes, I think that our problem is that having passed through the digitising process something might have happened at that stage. At least, we have received evidence that that was a matter on which we should be cautious, but you do not think that we should be?

(*Mr Damle*) My Lord Chairman, I believe that analogue is no longer safe in the same way that it was considered to be before.

Lord Brain] I think you are saying that we have got to be cautious of both.

Lord Tombs

354. In establishing the integrity of digital images I wonder how you rate the relative merit of procedural measures, for example, like management systems and audit trails and technological measures such as watermarking or encryption of digital signatures. Do you use both?

(*Mr Lazard*) My Lord Chairman, we use procedures at the moment.

355. But have you contemplated the technology? You mentioned watermarking?

(*Mr Lazard*) Yes

356. Encryption, limited access and that sort of thing?

(*Mr Lazard*) That has come into our consideration. It is not something that we are currently doing. We would be able to do that if it were found to be necessary, but again we prefer that there are procedures and we are following procedures that have been tested by BSI PD008 code of practice. We are wishing to follow that code of practice and these other methods we will be able to adopt, but we do not necessarily see that as needed now.

357. So that would it be fair to say that at the present time your needs are met by procedural methods?

4 December 1997]

MR PETER LAZARD, MR DILEEP DAMLE
AND MR MICHAEL URMSON

[Continued]

Lord Tombs *contd.*]

(Mr Lazard) Yes, my Lord Chairman.

358. But you have the capacity to add the others?

(Mr Lazard) Yes, we have the capacity, but we do keep the originals, so we do not feel that we need that defence at the moment.

359. Given the fact that you rely on procedures and for your purpose that is adequate, when we come to the use of such images in evidence, how would you like those procedures to be observed, by code of practice, by legislation or in some other way?

(Mr Lazard) By code of practice.

Baroness Hogg

360. What about where there is not an original in this sense, where you simply complete a record of an ATM transaction?

(Mr Lazard) If we are exchanging information with a third party, be that another organisation or an individual, then that is where we would look for additional measures. We would look for digital signatures or watermarks.

Chairman

361. I am intrigued in this response of yours. Looking at the future, more and more commercial activity, communication with government and other departments with yourselves are going to take place electronically and there may never be an original piece of paper, just to pick up Lady Hogg's earlier point. May I just press you further on that. Are you going to continue, as it were, to keep your feet firmly on the paper ground or do you believe that in time, as there is development—and, indeed, is your thinking within your organisation, your feeling about this—because of the growth of this electronic society sooner or later that paper foundation may have to be dispensed with? What I am really looking for here, Mr Lazard—and you obviously have got a very wide interest in this enormous amount of paper coming in, and I can understand the reason for handling it in the way that you do, and I can accept the archiving argument, at least for the moment—is whether you can share a vision of your future with us?

(Mr Lazard) We have only been talking about what we do with documents, with paper, with documents that start as paper. Ultimately one would see the removal of paper throughout the whole chain of events so that business is originated digitally and where we are in control, in other words, where we are working through that process from beginning to end dealing with the customer, we eliminate paper as much as possible. However, if a business transaction originates outside our own organisation, then we would want to see some form of encryption or some security applied to that transaction. Now that is the normal way that we would proceed. It is not really seen as part of the image debate.

362. But you do not see yourselves marketing on line?

(Mr Lazard) Yes, very much so, my Lord Chairman.

363. All right, so you attract my interest: do you still expect me to sign a piece of paper?

(Mr Lazard) No.

364. You do not?

(Mr Lazard) We are not steeped in paper, it is not by choice that we have paper; it is a requirement that we sometimes have paper and we need people to be able physically to sign documents and we need to keep documents with signatures. However, where we can remove paper from the process, then we have done so, and that has been a practice of ours for many years. Our branch procedures have very much removed paper.

Lord Tombs

365. Perhaps I may just follow up on that, my Lord Chairman. When you reach the promised land, Mr Lazard, and you do not have the comfort of a piece of paper as the original, the original is a created image, will you still rely on procedural controls or do you think that you will have to move to technological controls of the sort we have been discussing?

(Mr Lazard) Yes, I am struggling a little bit, because . . .

366. That gets us much closer to the legal thing that we are looking at.

(Mr Lazard) If you get rid of paper altogether, then you are not talking about watermarking images, you are not dealing in images any more, you are simply dealing in digital data, and to that extent we already have security measures in place and we will incorporate the ones that are appropriate to protect our own interest, and that is what it is really going to be about. It is further away from image processing really. It would not be seen as image processing.

367. Well, I wonder whether you will not create the missing piece of paper as a virtual image?!

(Mr Lazard) Oh, no!

368. As the original image.

(Mr Lazard) We may well be forced to do that by other legislation that requires us to hand back to customers a piece of paper that says, "This is what you told us, now sign it", so we may always need to produce a virtual document in that sense.

369. But the essential thing is that the original is now the image that you created, not a piece of paper?

(Mr Lazard) Yes.

370. The paper is a duplicate?

(Mr Lazard) Well, it is a duplicate until it is signed, and then it is a signed original.

Lord Brain

371. Electronically signed. If I may just pick up one that made me a little suspicious from what you just said, Mr Lazard, received electronically by telephone or from a computer a transaction from outside, you said then it did not need to be watermarked because you have received it, but how do you start the audit trail or how do you make sure that that piece of information is correctly identified as arriving from so-and-so? Subsequently you have got an original, as has been explained.

4 December 1997]MR PETER LAZARD, MR DILEEP DAMLE
AND MR MICHAEL URMSON[Continued

Lord Brain *contd.*]

(*Mr Lazard*) If it is an ATM transaction, then there would be no original document. We will have the records of the ATM transaction both as part of our ATM record and as part of our central mainframe audit trail, so that we will have a movement record maintained, but that is all digital. There are no images involved.

372. Yes, I quite agree, but how do we know that that original transaction is the original transaction, how do we know that the right thing was typed in somewhere? How do you know that it has been recorded and that somebody has not hacked into the line and done something that never occurred?

(*Mr Damle*) The fact of life, my Lord Chairman, is that as banks and as businesses we take a commercial judgment on the amount of risk that is involved. There has been an amount of speculation in the press about the degree to which hacking in respect of ATMs has been conducted. I cannot really confirm or deny those figures from my particular role in the bank. We do not suffer that degree of hacking. There might be the odd incident. In many cases customer disputes are resolved. If a customer says, I was not the one who withdrew from my account on that day, then a compromise is made.

373. It is cheaper to put a security system in.

(*Mr Damle*) There are some other instances, however, which might answer your question. For example, in telephony it is common practice now to record the conversation over the telephone.

374. And that, if you are using digital transmission, will also record not just the conversation but the digital pulses that have been sent down the line, if that is appropriate?

(*Mr Damle*) These two processes are currently separate, my Lord Chairman.

(*Mr Lazard*) Perhaps I may come in there, my Lord Chairman, and move your point on to the internet, which is far nearer in respect of the risk that you are talking about, it is far more obvious on the internet, then we would expect when we introduce internet banking that there will be a form of digital signature that will both authenticate the originator of the transaction and give us the ability to prevent any repudiation of that transaction, so that we have the twin benefits of non-repudiation and authentication through electronic security measures.

Chairman

375. Are there any other points? If not, Mr Lazard, Mr Damle, Mr Urmson, thank you very much indeed, you have been very helpful in responding to our questions. I do not know whether there is anything else that you or your colleagues would like to set before us, Mr Lazard, before we draw the session to a close?

(*Mr Lazard*) I do not think so, thank you, my Lord Chairman.

(*Mr Urmson*) My Lord Chairman, there is just one point, if I may. I have been involved in imaging for a number of years and when we started there was no guidance. I would like to emphasise that what we are really looking for is guidance, what we should be doing and what we should not be doing. As Mr Lazard has said, in terms of the things that are available, we can do them if we need to, but from a business point of view we need to know what we should be doing so that we are toeing the line, so to speak, and do not put our foot over the line.

376. That is a very interesting point. Do you have any feel as to what form that guidance should take? From your point of view are you looking for some form of statutory regulation, a code of practice?

(*Mr Urmson*) My Lord Chairman, anything that gives us the confidence that when we get to the questions we will get the right answers, whatever that form may take, and also to give the managers confidence to take that leap and start to move away from this paper culture that we are now in.

377. Yes, I understand that point.

(*Mr Lazard*) My Lord Chairman, if I may just add to that, what we would not want, of course, is to be burdened with over-elaborate security measures that far outweigh the risk to us, so that what we would like to see is a balance there.

378. I think that we are all very much aware that technology changes very rapidly and one is not ever, I think, going to try to tie it to any particular element of technology.

(*Mr Lazard*) And that is why the code of practice and procedures is to some extent more important to us, my Lord Chairman.

379. Again, thank you very much indeed.

(*Mr Lazard*) Thank you, my Lord Chairman.

THURSDAY 11 DECEMBER 1997

Present:

Brain, L.
Craig of Radley, L.
(Chairman)
Flowers, L.
Hogg, B.

Howie of Troon, L.
Kirkwood, L.
Nathan, L.
Tombs, L.

Memorandum by the Chief Constable's Office, Essex

I write in reply to your letter of 14 July seeking views on the presentation of digital images as evidence.

This issue has been examined by the Police Service in conjunction with the Home Office Police Scientific Development Branch (PSDB) in order to ensure the credibility of digital image evidence having regard to the ease by which such images can be manipulated.

In answer to the questions specifically posed in your letter I would make the following points.

1. The use of photographic imaging by the Police Service will undoubtedly grow over the years, particularly in regard to automated traffic enforcement systems and the spread of closed circuit television and video surveillance to prevent and detect crime and disorder.

The use of camera technology has proved extremely helpful in securing the conviction of offenders and in reducing Court time by the high incidence of guilty pleas in such cases.

2. The ease with which such images may be tampered with demands that strict technical and procedural rules be followed to ensure an audit trail sufficient to satisfy a court as to the authenticity of the evidence presented. Such specifications and procedures are set out in the attached Home Office and Association of Chief Police Officers (ACPO) publication 3/96 prepared in conjunction with the PSDB. (The author Dr S Lewis has, I understand, given evidence to your sub-committee).

3. The development of watermarking is seen as a possible means of avoiding the corruption of digital images. However, I understand that at the present time technical experts differ as to whether such a system can be "overcome". I do not know if Dr Lewis covered the issue in his oral evidence (he is currently on holiday) but I am aware that he has looked at the possibility of watermarking helping to ensure the credibility of images and would no doubt be willing to assist the Committee further if requested.

4. I am not sure what is covered by the expressions "modified" or "enhanced". The police have enhanced video images (not digital) in order to identify individuals, for example, in the course of the investigations into the Hysal Stadium disaster and the murder of James Bulger. In enhancing digital images it will be necessary for the forensic operative involved to explain to the Court how this was done and how the enhancement was still the original image. While such an enhancement could be described as a modification or alteration of the original if the operative can show nothing has been added to or taken away from the original image then I would trust that this would be acceptable evidence. Where however images have been modified in the sense of being altered I cannot see how such "evidence" could be held to be admissible.

5. Technologies which compress data or use error correction technology to raise problems but as outlined in the ACPO/PSDB publication 3/96 they can be overcome.

6. Surveillance cameras used in conjunction with image tracking do pose a threat to civil liberties if not properly regulated.

Many of the concerns surrounding the use of CCTV are addressed in the Local Government Information Unit (LGIU) publication, "A Watching Brief, A Code of Practice for CCTV." The cost of the document is £75. A working group consisting of ACPO, Metropolitan Police, Liberty and academic and independent technical experts, assisted in its compilation, together with Local Authorities. The Code sets out good working practices and it is recommended that it be adopted and all CCTV schemes include its guidance within their own 'code of practice'.

Any form of surveillance is an intrusion. The question to be asked is whether such intrusion is justified. The position is well set out in the preamble to the Council of Europe Recommendation (No.R(87)15) regulating the use of personal data in the police sector which states, "There is a need to strike a balance between the interests involved—the interests of the individuals and his right to privacy and the interest of Society in the prevention and suppression of criminal offences and the maintenance of public order".

In addressing the problems surrounding the developments in the field of both optical and acoustical surveillance techniques it is important to recognise the point made by James Michael in his book "Privacy and Human Rights", "Although technological advances have increased the threat to privacy from direct

*11 December 1997]**[Continued]*

surveillance, it is modern data processing that presents the greater threat to privacy for populations in general”.

7. The Police Service have long recognised that if the public are to have confidence in the police use of such technology and to allow its continued use and development then regulation and subsequent audit is necessary.

In this context ACPOs Code of Practice for the Police Use of Computers, the drawing up of guidelines for the use of CCTV and the technical specifications and procedures for automated traffic enforcement underline our commitment to control and monitoring. In addition the current work being undertaken by an ACPO working group under my chairmanship in drawing up a comprehensive paper setting out the Police stance on privacy and the control of surveillance technology which will be widely circulated is in order to inform the public and sustain public confidence in the use of such technology.

It is against this background that the Police Service would also encourage legislation regulating surveillance technology and governing the unauthorised disclosure of information so obtained.

8. All police officers and civil staff members of the Service are aware of the provisions of the Data Protection Act 1984 and the ready availability of the Code of Practice, together with operating and audit manuals results in a high degree of awareness. In regard to surveillance the requirement to seek senior officer approval before the deployment of surveillance equipment ensures that improper use is avoided and that when used it is closely supervised. The paper currently being prepared and referred to in answer to question 7 will also assist in providing an ethical basis for officers contemplating surveillance and the criteria to be considered before authorising its use and the disclosure of material so obtained.

9. I am hesitant to enter into the minefield of media publication but if “modified” is synonymous with “altered” the short answer is, yes there is a need for special measures.

John H Burrow

Chief Constable, Chairman, ACPO
Working Group on Data Protection

5 August 1997

ENFORCEMENT TECHNOLOGY NATIONAL GUIDANCE MANUAL

The Use of Front Photography in Road Traffic Enforcement

Since 1991 the expansion in the use of unmanned and manned devices which record the circumstances of offences of excess speed or red light running on a photograph, video or digital image has been one of the key factors in the role of using enforcement to reduce death and injury on the roads.

The use of such devices was the subject of extensive discussion during the passage of the Road Traffic Act 1991 and much debate centred around the perceived intrusiveness of this type of equipment into the privacy of the occupants of a vehicle when an image of that vehicle was recorded. At the time of those discussions, rear photography of offending vehicles was the best technical option, and the fact that drivers would not be identified from such photographs possibly allayed any public disquiet and gave acceptance to the procedure of identification of offenders by enquiry through the registered vehicle keeper record.

A number of police forces in England and Wales have used unmanned devices for several years and each has identified problems with the current process of identifying offenders. Apart from problems relating to the identification of vehicle class when large goods vehicles are recorded from the rear, or when number plates are partially or completely obliterated by loads carried on private cars, there are problems which relate to the use of unregistered vehicles or those vehicles where transfers of registered keepers have not been notified.

One of the areas of concern centres around the actual identification of the offender once the presence of a vehicle at the locus is agreed by the registered keeper. It is not uncommon to receive replies from registered keepers indicating that one or more persons could have been driving the vehicle on the day concerned and asking the police to be more specific as to the age and sex of the driver. They, the keeper, may then be able to identify the driver to the police.

The use of front photography, or simultaneous front and rear photography, may reduce the difficulties in driver identification but it is recognised that some people may see its application as an intrusion into privacy and of official surveillance of everyday living. For that reason the following protocol has been drafted by the ACPO(T) Traffic Enforcement Technology Sub-Committee and any force which uses or considers the use of front or simultaneous photography must adhere to its principles.

The use of any image, recorded by a Type Approved enforcement camera, will primarily be for the prosecution of the offence of excess speed or red light running which it records. It must be recognised that sometimes images will record the presence of persons in a motor vehicle which will be prima facie evidence of their involvement in connection with another offence such as taking without consent, aggravated vehicle taking, theft, driving whilst disqualified etc. Also, in addition to traffic related offences, the image may record

11 December 1997]

[Continued

the occupants of a vehicle making off from the scene of another serious offence. It would not be right to have such potential evidence available and not use it in the investigation of these offences.

The use of the protocol will make it clear to the public at large that technological assistance and image recording is a fundamental part of the enforcement of traffic legislation in an effort to reduce death and injury on the roads and is not a complex surveillance system provided to allow official intrusion into the private life of individuals.

PROTOCOL

The identification of any offender, whose alleged offence has been image recorded by a Type Approved enforcement camera, will normally be accomplished by application to the registered keeper of the vehicle to nominate the driver of the vehicle under Section 172 of the Road Traffic Act 1988.

An open approach to these enquiries will militate against mistaken or maliciously misleading responses which would otherwise lead to more serious investigation relating to perverting the course of justice.

When front photography has been used:

- The registered keeper will be told at the time of the initial enquiry that the offence has been photographed (as at present) and that the record contains detail that may assist with the identification of the driver.
- A copy of the photograph will not be sent at this stage.
- Should the registered keeper nominate another person, then that person will also be advised at the time of first contact, that the image contains detail that may confirm the identity of the driver.
- Where it appears that an image or series of images may contain prima facie evidence relating to any other serious offence then the examination of those images is sanctioned for that specific purpose. The subsequent use of any image as evidence or part of an identification process is governed by the Police and Criminal Evidence Act 1985.
- Any potential defendant, in respect of a speed or red light offence, should be given the opportunity of viewing the image in the same way as current procedures.
- The displayed image will only show that part of the vehicle which permits the identification of the driver with the remainder of the passenger compartment obscured.

The initial image, recorded by the device, will always remain in its total and unaltered condition as the "best evidence" for subsequent production in Court if necessary.

Examination of Witnesses

MR JOHN BURROW, Chief of Police, Essex and MR JOHN BLACK, Data Protection Officer, Essex Police, called in and examined.

Chairman

380. Good morning, Mr Burrow and Mr Black. Thank you very much for coming to see us. Also thank you for your very helpful written evidence which we have studied and found very useful. As you know, we are looking into a variety of topics surrounding the title Digital Images as Evidence and there is a number of areas we would like particularly to concentrate on as you will know from the oral questions which I think you will have had a copy of. Before we start, might I invite you to introduce yourself and your colleague for the record. If you want to say anything by way of kicking us off we will be very pleased to hear it.

(*Mr Burrow*) I am John Burrow, the Chief Constable of Essex and the Chairman of the Association of Chief Police Officers' Working Group on Data Protection. I have with me John Black who is the Secretary of that Working Group and he has a greater detailed knowledge than I have. Any difficult questions I shall refer to Mr Black! You gave some indication as to the line of enquiry you may take this morning. It is interesting that I was attending an international conference on privacy in Montreal recently and I was asked to speak on two television

programmes because of the surprise in Canada that we—the British public—allowed such extensive use of CCTV. "Surely, Chief Constable, this is an intrusion into people's privacy? How do you manage to have such a widespread use of CCTV?" Of course, the answer is that there is strong public pressure, at the moment, for CCTV systems. It gives a greater feeling of assurance, women use multi-story car parks much more frequently because they know there is CCTV surveillance. Small towns with relatively low records of crime nevertheless demand that CCTV is introduced. That is the balance, of which I spoke in my paper, between the right of the individual to a freedom of privacy and the right of an individual to go about his business unmolested. It is the question of balance which I think has got to be struck. I think in determining that balance—and no doubt I will return to this in the course of the morning—who in fact sets that balance, who in fact determines whether the public good should indeed overrule the right to privacy of the individual. At the moment, I think that balance is about right, I think there is public confidence in the use of CCTV but I would feel that that confidence is fragile and could be reversed. I think the effectiveness and the advantages of CCTV could be lost then. I think that would be to

11 December 1997]

MR JOHN BURROW AND MR JOHN BLACK

[Continued]

Chairman *contd.*]

the detriment of the public at large and therefore in developing my case further this morning I will be advocating for stricter control of CCTV in order to retain that public confidence in the longer term. I think that is all I need to say Lord Chairman.

381. That is very helpful because it does go very much to the heart of some of the concerns which have been expressed to us and which interest us around this table. Could I take you a bit further, going on to the first question but taking it a bit further and looking at just what you said. The first point was the confidence it gives to the public that these surveillance systems are likely to reduce the risks they run of suffering some injury or crime but in your experience—and we have seen some of the images which these systems produce—a lot of that imagery is not useable as evidence, it does not have the definition or it cannot be used in that way. Your interest then in it is as a deterrent to crime entirely or do you believe it does have use evidentially?

(*Mr Burrow*) I think certainly it has a use evidentially. I think systems are improving, the level of definition has improved significantly. There is also, however, a need for people who use CCTV to properly maintain their equipment and to change the film. Members may recall the very blurred images which were produced in the wake of the Jamie Bulger case in Liverpool where the shopping precinct which captured on tape the boy being led away was extremely poor because the film had been used and reused, there was dust on the lens, the general maintenance was poor. If the systems use modern technology and are properly maintained, the level of imagery is good and can be used in evidence. The town of Colchester six months ago launched their CCTV system, one of the most extensive—indeed I think Colchester would claim the most extensive—uses of cameras in a town centre. In that six months, the police have viewed 114 video tapes and of that 114 they have used them as evidence in 44 cases. So the images have improved over years and with proper maintenance they can be used so there is a very real benefit to the police in using CCTV captured images. The second part of your question though as to the general deterrent value I think is significant. Again, if I refer to the Colchester position, in October the number of cars stolen from municipal car parks fell from something like 46 in the month of October 1996 to ten and I think that is a continuing reduction, consequently people are more willing to use those car parks knowing that they are under surveillance and so on. There is a further extension in the town of Brentwood, women travelling particularly at night can telephone the centre and their passage across the town will be monitored by cameras throughout their walk through the town and again giving an assurance to individuals. I think on both scores I would not wish to diminish one or the other, saying it is extremely useful in evidential purposes provided the equipment is of a kind and is properly maintained but also it has a significant impact on the general public giving a feeling of assurance. With the introduction of the scheme in Colchester they asked MORI—the poll people—to ask the local community what they thought about it. The enquiry, which was undertaken in September, has only

recently been published. If I can just mention three of the questions that were posed. They asked the people did they know that there were cameras in the town and 81 per cent said yes they did. “Did it make you feel more safe?” and 52 per cent of the people said yes it did. No-one felt that it made them feel less safe, although 45 per cent said they did not think it made any difference but it has only been going for six months. Asked if they would wish to see such a system extended, there was strong support for such an extension by 59 per cent and a tendency to support by a further 31 per cent and those strongly opposing or tending to oppose any further extension, three per cent. It was not as if the people did not know, 81 per cent knew there were cameras there. Over half of them felt that they felt safer, the very issue you raised, my Lord, and then the support for its further extension was again strong.

Lord Howie of Troon

382. I was interested in what you said about Toronto since on the new motorway, route 407, to the north of Toronto through the outskirts CCTV is being used there for the purposes of road pricing. That is images are taken on the slip roads leading on to the motorway with the intention of billing these people for the use of the motorway. Would you be happy if images obtained for that purpose, that is for road pricing, were then used for other evidential purposes?

(*Mr Burrow*) Yes, I would. I think what you would need to do is in any control of the system you would say that the purpose for which that system was introduced was for road pricing, in the example that you give. It would be possible for the police in the prevention of crime and the apprehension of offenders to seek access to that system. Now if in fact you were to say “We want other persons to have access” then it would be for you to determine the propriety of those other persons having access. As part of the legislature, you may say “No we do not want the police to have access to those systems” and I come back to the point I made earlier, that is a matter of public policy that you must decide. I would be of a view that disclosure for the prevention of crime or the apprehension of offenders [if we felt that] was important, if there was the passage of a lorry, which we know in terms of the explosion which occurred at Canary Wharf, that the lorry was bought in a particular area, it was moved to another area and then brought down to London, we might say we would wish to have access to such a system to monitor the progress of the vehicle and see what its movements were.

Chairman

383. If a defendant wanted access to that sort of material in order to prove perhaps that he was not there or had been in another place at the time he was alleged to have committed a crime, what would the police feel about that?

(*Mr Burrow*) There are two things there. First of all, the rules on disclosure would require you, if you were using that as evidence against the defendant, to

11 December 1997]

MR JOHN BURROW AND MR JOHN BLACK

[Continued]

Chairman *contd.*]

disclose that evidence to him. In fact, if you were carrying out the investigation and he asked then for subject access, provided CCTV systems come within the New Data Protection Act—and there are indications because of the wider definition, it is not limited to the automatic processing of data by relation to the individual and consequently the likelihood is that CCTV systems will be embraced in the new law—then the subject could ask for access, provided it was not at that stage going to inhibit a police investigation he would be entitled to such access.

Lord Brain

384. Three quick questions. Who is running the system in Colchester and in Brentwood: is it the police, the local council or some independent body?

(*Mr Burrow*) It is the local authority who have ownership of the system both in Brentwood and in Colchester. In introducing the system they had and were in close co-operation with the police and also took advice from the Local Government Information Unit. You may have seen that they have introduced a code of practice.

385. The second one is that therefore it was the local council that set the standard of camera, lens and other procedures, do they have routine checking procedures, for example, of colour balance on their cameras because if you were using film, all film is checked before it is ever dispatched and you know what the colour balance is.

(*Mr Burrow*) They do carry out checks. I understand later this morning you will be speaking to a group from the Home Office which includes Mr Jim Aldridge. Mr Aldridge will take great pride in producing his ROTAKIN as he calls it which is a system rather like a test card.

386. The final question is I live in Devon, Exeter said recently it is installing a system and the newspaper says that they will install number plate identification for use on the system. We have seen this system in the City of London.

(*Mr Burrow*) Yes.

387. Has Colchester got it? If it is the local council system, how does one get a cross-check with the stolen car records on some computer because it implied in the newspaper that the local council will ring up the police when they get the alert on the car identification and not the other way round.

(*Mr Burrow*) I think there has to be a difference drawn. I would doubt very much that a local authority would have a system similar to that in the City of London of an automatic number plate retrieval system.

388. The newspaper indicated they had, that is hearsay.

(*Mr Burrow*) That system (the City of London) has direct access to the police national computer and we would not allow that by a local authority, that would be quite clear.

Lord Brain] I will inquire further.

Lord Kirkwood

389. I would just like to go back to the use of traffic evidence for other purposes. In the protocol that you included with your written evidence it says "Where it appears that an image or series of images may contain prime facie evidence relating to any other serious offence then the examination of those images is sanctioned for that specific purpose". Who initiates that process? In other words, is there someone looking through all these traffic offence pictures and suddenly they spot an odd criminal or is it retrospective, if something happens subsequently they then go back and look at the evidence available. There is a problem there of Big Brother a little bit, someone looking through photographs to spot criminals. Is that the way it happens or am I misconstruing?

(*Mr Burrow*) I think the volume would preclude that sort of scanning on the range that you speak of. What you would find probably was that there was suspicion of an offence at something like 10 o'clock on Thursday morning and then probably you would have a protocol within each force that in order to go back and check you would need the authority of the inspector or someone in the rank structure. I would be a little hesitant because clearly the Metropolitan Police may say a superintendent, in Cumbria they may say an inspector because of the availability but you would need authority to retrospectively check that film.

390. Are you satisfied with that system in general?

(*Mr Burrow*) Yes.

391. Whatever the protocol is, you would not want to make it uniform throughout the country?

(*Mr Burrow*) I think in the light of your question I can see a difficulty could arise. I would be prepared to go back and look at the Association of Chief Police Officers' Code for use of computers bearing in mind we are talking about CCTV which is not covered currently by the Data Protection Act and ask ourselves whether in fact we need to make it a specific issue. For example, within the computer field, if you have a major enquiry, that major enquiry is then kept, retained and archived. If anyone wants to go back to look at that archived material they must get the authority of an assistant chief constable, that is written into our current code. In view of the question, I think we would need in the wake of the New Data Protection Act, which in all probability will embrace CCTV, to amend our code in the light of that new legislation. Then I think the very question you raise needs to be asked [there] as to whether we give a level of supervision to ensure that is conformed with.

Lord Tombs

392. Mr Burrow, you have mentioned a rather striking figure of a fall in car theft from 46 to ten following the introduction of CCTV. Was that accompanied by an increase in successful prosecutions or was it simply a deterrent and if the latter did the potential car thieves turn their attention to street parked cars I wonder?

(*Mr Burrow*) I cannot answer the first question as to how many prosecutions followed as a result of

11 December 1997]

MR JOHN BURROW AND MR JOHN BLACK

[Continued]

Lord Tombs *contd.*]

CCTV. I would suggest, however, that it is largely a deterrent value. I cite that one because it is particularly graphic but there has been a fall across all crimes within the Colchester town centre. It is interesting when one looks at Chelmsford, which has had a system for a little longer, recorded crimes of violence have gone up. When we ask about that, it is because we get there sooner and we are aware of violence now being committed that we were not aware of previously. I think the general point is that the number of offences has dropped across the whole range. It is not a drop here but an increase there. Sometimes the question is posed "But have you merely displaced crime to the surrounding area?" and again in Brentwood where the system has been in operation for some four years and in places like King's Lynn and Airdrie in Scotland where they have been in existence for far longer, there is no evidence to suggest that there is a displacement of any significant proportion outside the town centre covered by CCTV.

Lord Flowers

393. I wanted to ask Mr Burrow question two or something like it about public attitudes to surveillance systems. You have answered very largely what I was going to ask you in your opening statement but I would like to push you a little bit further if I may. Do you really consider that the public have taken a conscious decision to accept CCTV systems or is it really a result of a [lack of] ignorance on their part? For instance, are they aware that CCTV systems are not regulated? No doubt in the police force you apply a certain amount of self-discipline but there are many private systems also, some of which you have mentioned yourself, which are unregulated, certainly statutorily so, so they may be misused. Are they aware that images can be modified to make them represent something which was not the case originally at all and done quite easily what is more? Are they aware that at least with private systems information gained from surveillance can be given or sold to the media? Now if the public is aware of that sort of thing do you think you would still have the same degree of public acceptance? If you think they would be worried, is that a case for having some strong regulation as soon as possible?

(*Mr Burrow*) They are not aware. They are aware that the systems exist, they can see the cameras, there are the notices and what have you as to what the system is and who owns it and so on but of the other points that you raise, no they are not aware. This is my cause for concern, I feel that when they become aware, either through celebrated court cases or whatever, then I think there will be a falling off of that public confidence and their willingness to see the continuance of close circuit television. Some of you may be aware of a recent court case where a Mr Peck in Brentwood was captured on the CCTV system attempting to commit suicide. He was in the road with a knife attempting to slash his wrists. Brentwood were quite pleased with this because immediately they alerted the police and on the tape you see the two police officers arriving, hesitantly approaching the man with his knife, getting hold of

him and then, realising that he is suffering from some mental disorder and attempting to commit suicide in a state of depression, they got him to hospital. Brentwood then subsequently disclosed that film to the BBC saying [just] what a wonderful thing, CCTV had saved this man's life in all probability. Mr Peck was not pleased with seeing his picture on BBC and he came to the High Court to seek a judicial review. It is interesting to note, I have not got a copy of the Law Report, but both the Independent Television Commission and the Broadcasting Standards Commission agreed that through human error the privacy of Mr Peck had been infringed. Yesterday, sitting in the High Court, Mr Justice Harrison dismissed the application, there was no breach of the law. Now, that is the very issue that you raise, if we do not have regulation. Again it will be a matter for yourselves as to what you believe that regulation should be, my view is there ought to be regulation. In 1984 the Home Office hinted that they were considering regulation of CCTV and 13 years later we still do not have any regulation. Now it may well be that they will argue that the New Data Protection Act with its wider cover will embrace CCTV but what are we going to get in the new legislation? Are codes of conduct to be made mandatory? Are we going to have voluntary codes which I think would not answer the very issue that you raise. Briefly, I believe there ought to be regulation. Whilst the local authorities I think have observed their voluntary code which is very detailed, there is a whole host of people who use CCTV who do not abide by that code and undermining public confidence in one area will extend across the whole area and therefore I am anxious to see some greater control.

Lord Flowers] That is exceedingly helpful. I would like to ask Mr Burrow, in spite of his modesty in this respect, what sort of regulation he would like to see? You may prefer to take that later, my Lord Chairman.

Chairman

394. I think while we are on it, I was going to ask the question myself but as it has been asked perhaps you would like to respond Mr Burrow?

(*Mr Burrow*) I think, first of all, there ought to be regulation that people who operate CCTV systems must abide by a mandatory code of practice. I think there ought to be the provision where a Registrar or Commissioner, as he or she will be called, has the right to audit. I do not expect that audit to be on a weekly, a monthly or even a yearly basis but I do hope that the Registrar has the ability to go in and look at a system to see that there is compliance with the regulation. In other words, not to wait for a subject to complain that they believe their rights have been infringed but for her to take proactive measures to ensure that people are complying with that code of practice. I am not at all dismissive of the argument that codes of practice are more detailed than the principles. The principle of fair obtaining, what does that mean in terms of the bank system or the little corner shop that has a system? I think, therefore, the code of practice needs to be widely drafted. I think any measure less than that would leave it open for

11 December 1997]

MR JOHN BURROW AND MR JOHN BLACK

[Continued]

Chairman *contd.*]

those who seek to abuse the system to abuse it and thereby possibly lose public confidence with all the results that I have mentioned.

Baroness Hogg

395. With reference to the specific example you gave us a moment ago of the release of CCTV video and the attempt to commit suicide, do you think that a code of practice should forbid the police to release to the media such material?

(*Mr Burrow*) Yes. I think what would be said. [therefore, is] What is the reason for having your CCTV system? It is for road pricing, it is to prevent shop lifting, it is to do this or that. Release for other purposes would be forbidden. There is an interesting disclosure which [no doubt] your Lordships may have seen on bad driving on motorways which has been shown on tv.

396. Yes.

(*Mr Burrow*) Largely, I feel, for entertainment purposes. No, no, no it is argued it is for accident prevention purposes.

397. Cheap television.

(*Mr Burrow*) But I must admit that my colleagues are somewhat divided as to whether the police should hand over film to tv companies to show in that way. There are those arguing "this is good accident prevention" release, whilst there are those saying "no, we are arguing that other people should not release film to tv companies and here we are doing the very thing that we are deploring other people doing".

398. Exactly.

(*Mr Burrow*) I speak for myself and not for my Association when I say I would wish to see that being very tightly controlled. The classic example was this last weekend where the camera at the Basildon Maternity Hospital captured the image of the young woman stealing a baby and, of course, it was that image on television which prompted people to ring in and eventually ensured that we were able to return the baby to the rightful mother. There are circumstances where it is quite proper to disclose but I think that generally, which I think was the thrust of your question, no I would not agree with wider disclosure.

Chairman] This remains at the moment a decision at Chief Constable level or is there a Home Office guidance?

Baroness Hogg

399. Or below that.

(*Mr Burrow*) It was the Chief Constables who decided that they would release to the press or to the tv companies.

Chairman

400. Is there a financial transaction involved in that?

(*Mr Burrow*) Yes.

Lord Howie of Troon

401. With regard to regulation and public information, would it satisfy you if the user, whether it was the hospital or a big store or a corner shop, exhibited a notice in a prominent place saying "surveillance cameras are in use on these premises" under the terms of whatever code of practice was adopted? Would that satisfy you?

(*Mr Burrow*) Yes, provided the code of practice was agreed.

Baroness Hogg

402. I just want to make sure that I understand that answer. Was the implication of your answer that it would satisfy you that the material could then be released in any circumstances?

(*Mr Burrow*) No. I think what it would be is that there would be a notice alerting people that there was a CCTV system, that the ownership was with the store or hospital and that there was a sentence at the bottom saying "further information can be obtained from the Registrar" and a telephone number.

403. The implication from such a notice would not be that you could see yourself on cable tv in three days' time?

(*Mr Burrow*) No, no, no. Indeed there would be a code of practice which would be mandatory, to follow my line of argument, and in fact the general public would know that except in the most exceptional circumstances the corner shop could not release such images to anyone else.

404. I think it is worth exploring this point because there will be an increasing demand for cheap television and an increasing number of companies putting material on and a symbiotic relationship can develop between the police and television company that want this material. I share your caution, I think it can be very seductive.

(*Mr Burrow*) Hence my stance on disclosure that it would be in the most exceptional circumstances. I referred to the hospital incident last weekend as exceptional circumstances. [I think the] General release I would be opposed to.

Chairman

405. Talking about the code of practice and whether these systems are publicly owned as opposed to installed under contract to a public authority, do you see any distinction as to the public acceptance whether there is public ownership or whether they are installed, as of course many corner shops will be done, by a contractor?

(*Mr Burrow*) I think, rather like the Data Protection Act, it is the person who owns the data, not the person who owns the equipment, who should be tasked with complying with the code. I think you heard when talking of digital imaging of certain requirements that we would look for to give confidence in the courts in the evidential chain that images had not been interfered with. I feel that would impinge on contractors supplying systems, that they comply with that requirement. On the general rule I

11 December 1997]

MR JOHN BURROW AND MR JOHN BLACK

[Continued]

Chairman *contd.*]

think it is the person who owns the image who should be the person who is responsible and accountable.

Lord Tombs

406. It has been suggested to us in evidence, Mr Burrow, that city centre surveillance systems can be quite effective in deterring petty crime and anti-social behaviour but they are not very effective in the pursuance of serious crime. Would that be your experience?

(*Mr Burrow*) The Harrods bombers were caught by CCTV. You cannot get a more serious offence than terrorism. I think it is right that in fact the majority of cases are ones of assault, are of criminal damage, shop lifting. It is interesting that we capture quite a number of drug deals and I think that is up in the serious level. There are instances which I could cite of robberies being seen in process and persons being arrested. It would be wrong to say there is a high incidence of very serious crimes which are captured, solved, by closed circuit tv, but there are some. I think you also have to ask yourself how many bank raids have been thwarted by the fact that the cameras are there.

407. The second question, I wonder whether in Essex you have looked at the rather academic question of the cost benefit relationship between closed circuit systems in town centres and their costs? I mean tangibly, not the feeling of goodwill that arises.

(*Mr Burrow*) I would like to do some work on that. I think we ought to try harder rather than just the anecdotal evidence that we currently have. Speaking to the Divisional Commander responsible for Chelmsford town centre, and I think, John Black, we have got some figures as to the cost, the Chelmsford system cost £500,000 to set up, the running costs are £160,000 per year, of which the staff take the largest proportion obviously, some £120,000, and then maintenance and others £40,000. So having set the thing up at a cost of half a million, generously aided by grant from Government—The Colchester one is 1.3 million. There are very, very significant costs.

408. Indeed.

(*Mr Burrow*) Talking to the Superintendent at Chelmsford, he was saying that quite often coming in on a Monday morning the criminal damage in the town centre with plate glass windows being broken could well exceed £20,000, that would be quite commonplace. That has virtually ended. I remember certainly within the first month they had captured on TV a man who threw three glass beer bottles through three plate glass windows and immediately you are saying you are recovering some of that £160,000 per year. Then, of course, the cost that you talk about of goodwill, a greater number of people coming into the town centre to do retail business, more people feeling that they can come in for leisure pursuits and so on. Certainly talking to the Chief Executive of Chelmsford he is more than satisfied that he is getting good value for money. It would be interesting if we could persuade one of the universities or research institutes to do a more indepth survey rather than just relying, as I have done, on anecdotal contact.

409. That might be quite useful in public relations to have such a research study done. You have made a persuasive case for the insurance companies paying for these systems.

(*Mr Burrow*) Well, of course, you will be aware that the Government's grants for the introduction of CCTV were always based on private money, public money as well, but local money contributing to the whole. I am aware, certainly in Colchester, that the insurance companies contributed significantly to the overall cost.

Lord Kirkwood

410. I think the Chief Constable has actually answered most of the points that I was going to put forward about whether voluntary codes are sufficient. Perhaps I could just add one small point. Would you see the use of law requiring a licensing system? How would it be carried out in practice? Do you think the licensing of the use of CCTV cameras is an appropriate way to go forward?

(*Mr Burrow*) I am aware, and indeed in the Local Government Information Unit's code, they talk of progressing beyond the voluntary and they refer to licensing. One could say that local authorities would refer to licensing because there would obviously be a cost element and a little income generation is no bad thing. I am not convinced myself that there needs to be a licensing system. I think, in fact, the proliferation of CCTV would make that somewhat cumbersome. What control would licensing create? I think if you were moving to a lesser legal framework than what I am proposing then licensing may be an intermediary step. I must admit that I am not convinced that licensing is going to add much if you have a regulation with a mandatory code.

411. I was not thinking of licensing through the local authority but that the local authority themselves would be licensed by some government office, something rather like Swansea car licensing.

(*Mr Burrow*) The Government might be attracted to that idea.

412. Once again there has got to be a commonality about the code of practice. This would be better dealt with by a national office.

(*Mr Burrow*) I think the issue of whether in fact the Commissioner for Data Protection would ask for registration, albeit I am aware that the present Registrar is herself worried about whether there is registration of all systems that currently exist. It would be much, much wider if, in fact, the corner shop with its CCTV system then had to inform the Registrar. I would much prefer, as I say, a proactive audit arrangement whereby the Registrar would have a team of people who could go into the corner shop, ask whether in fact a CCTV system was operating and then check that it followed what might be called the retail element of the mandatory code.

413. And the consequence if they were not carrying that out would be that they would be legally prosecuted?

(*Mr Burrow*) Indeed they would, yes.

11 December 1997]

MR JOHN BURROW AND MR JOHN BLACK

[Continued

Baroness Hogg

414. I think this leads to the next set of issues which we want to raise which is what happens in court. There is a high incidence of guilty pleas at the moment. In your view to what extent does that rest on a lack of knowledge by those who are prosecuted of how easy it is to manipulate and alter digital images? One could imagine once that knowledge permeates it having two effects: one, a greater willingness to challenge the evidence and, secondly, a downward spiral in confidence as to the prosecution process. Are we living on borrowed time with this technology in the legal process?

(*Mr Burrow*) I think the question that you pose will become more significant as we move from tape video to digital imaging. You are aware from evidence that has been given to you previously of the ease with which digital images can be manipulated. The present arrangement provided, and indeed most authorities, certainly public authorities, have a code of practice whereby the video tape can be evidentially proved from the moment it is taken to the moment that it is produced in court. I am also told that forensic experts are adept at being able to say whether a tape has been interfered with if in fact it was claimed that it had been manipulated in any way. The courts could would then have confidence. Let me say at the present time that I have never found barristers short of being able to challenge evidence and if in fact it was challengeable at the moment then they would do so. Because of the points that I was making about the audit trail from the capture to its presentation in court, the difficulty of altering that without it being recognisable, there is very little challenge at present. The question as to whether in fact it would be easier to challenge digital images and to such challenge accepted by a jury or the magistrate I think is something that we are looking to. Again, we would be relying on the trail: who took the photograph, how was it passed to the police, who in fact had handled it and so on? We would have to examine that trail to ensure that all the steps had been taken and there was no opportunity for people to manipulate the image. Again you are aware that with digital imaging one of the values is you do not have film, you do not have to change it, it is transmitted automatically to the centre. Could it be interfered with during that movement across what is most likely to be a public network? Again there have been specifications drawn up which would ensure that that image was encrypted and therefore the likelihood of it being manipulated in transit would be eliminated. Other steps as to how you would handle it within the police before bringing it to court I think would be necessary to give confidence. I do acknowledge that there could be challenges and how effective those challenges would be we will need to wait and see. I think we will be making every effort to ensure that we can satisfy the court that from the moment of capture to the moment of presentation in court we have guarded that image all the way to give public confidence and credibility to that evidence. It is going to be more difficult.

Lord Brain

415. Pursuing that one slightly and then going on slightly wider. Do you think that if the system was designed so that when the image is taken and

encrypted in parallel with that, and perhaps by independent means, data of the time, place, similar sorts of information are sent down a line and recorded in parallel rather than on the same piece of information would be a good idea?

(*Mr Burrow*) That has not been put to me previously but I can see the benefit of that. Would the two pieces of information be received at the same place?

416. I think that is a question of systems design. Probably the same place but possibly not necessarily on the same piece of equipment. I do not want to pursue that further. I was going to pursue a little bit more how do you present this information in court. Is guidance and indication the best way or should there be a sort of routine procedure—you have talked about an audit trail—that when somebody goes into court they do not have to be asked to produce the audit trail, in their evidence in chief they give an indication of where the image came from and the parallel information as to who took it, the time, the place or whatever?

(*Mr Burrow*) Yes, I think it would be required by the court for them to say “if you are going to produce this image we need to be satisfied when it was taken, how it was then held” such as you would do with a voice recording which we now take from a prisoner. In fact we then say the master tape was sealed in the presence of the prisoner and the seal has not been broken until it comes into court and so on. Yes, you would have to prove that case.

417. In the current system you would say “right, this video tape was taken from such and such a room in Colchester which is a secure room, put in an envelope and put in a safe” and so on?

(*Mr Burrow*) That is right.

418. One would need to do the same with digital with some form of write once memory so that again although there might be in the memory of the whole system a working copy there is a master copy that is held securely on video or whatever it is until the evidence is required.

(*Mr Burrow*) Yes.

419. That needs to be written into some form of system management for presenting evidence. Is that your opinion?

(*Mr Burrow*) Yes, indeed, just that.

Chairman

420. Mr Burrow, in your written evidence you draw our attention to the impact on privacy of data processing and you quote indeed from the *Privacy and Human Rights* book on that. Data processing presents a very great or potentially a very great danger to privacy. In the remaining few minutes, I wonder if you would like to talk a little bit to us about that because clearly with data processing techniques and technology on face-matching, data information in one store can be compared with material elsewhere. What is your view about that insofar as it may impact either on the value it will give to you in prosecuting and following up information and taking cases to court or in terms of the public concern about the invasion of privacy? Could you give us a feel for how you see that?

11 December 1997]

MR JOHN BURROW AND MR JOHN BLACK

[Continued

Chairman *contd.*]

(*Mr Burrow*) The point made was that initially people were concerned and one recalls the Younger Committee and then the Lindop Committee looking at privacy and data protection and that it was computers and databases that needed to be controlled. Then there was a period where it was thought, "Well, that is all right. We are fairly happy with that, we have the Data Protection Act", but it is intrusive surveillance which is the problem. It is CCTV, it is audio surveillance, it is these issues which are now top of the agenda and I think we have now said, "No, it is the combination of the two", and one looks, for instance, at automatic number-plate reading whereby yes, we have got a machine that can read a number automatically, but it is the ability then in looking over a period of weeks at a million cars going through the City of London and checking them against a 40 million database. No one could do that, but a computer can do it in microseconds and by the time the car is leaving the City after a mile, the officers are stopping it because it is recorded as stolen or whatever. The road pricing system that you speak of, there may be a lot of people who would be very interested in the certain passage of certain motor vehicles, but is that the purpose, and yet the ability of computers to store and then analyse that information against an individual's details is, I think, a trend which needs to be controlled and I think there is a need for there to be awareness by the general public of just what is now capable of being done by the use of surveillance linked to computers which requires the regulation of which I speak. Reverting to an earlier question, I think there is a degree of ignorance as to what can be achieved. When that ignorance is replaced by awareness, then it may well be that there will be a falling off of public confidence in the public authorities having control of such systems. Therefore, I think we should be ahead of the game and be looking at a greater degree of regulation to ensure that when that greater awareness comes about, there is still confidence that public authorities will be using, and indeed not just public authorities, but people in general, will be using surveillance and computer databases properly as controlled by the legislators who have determined what is in the public interest and what is a private right.

Lord Flowers

421. Would you be worried about these technologies being used, well, they are being used, in crowd control if you also had the ability to search a database for facial recognition?

(*Mr Burrow*) I have had a long discussion on facial recognition and I understand that the American Pentagon are probably the foremost experts in this field. If in fact you have a compliant person who stands in front of the camera with a normal face and the photograph is taken and then you contrast it against the database, that is achievable now, and the one-to-one comparison. To do it against a crowd, they say, is years away. The turn of the head, the use of make-up, the ageing process against the original image, all of those circumstances make it very difficult. Experiments have been carried out and, as I say, the Americans have looked at all the systems which are currently in being and not for the first time the technologists are claiming that their system can do this, this and this, but in actual fact they have not been able to find a system which with any degree of precision enables them to do it randomly in a public order situation. There is a system at Heathrow, I believe, which is done when the person checks in and then because it is an internal flight no passport is shown and the person at the boarding gate looks at the image of the person who checked in to ensure that they are the same person. I think what has happened, and indeed I was under the misapprehension at a time when people said, "Oh well, they have got a facial image system at Heathrow Airport", and when you enquire of it, it is the system of which I speak, which is not what you had in mind where you can in fact scan people entering the City of London and say, "He's a known terrorist", or whatever. That is not capable of being undertaken at the present time.

Chairman

422. Well, Mr Burrow, time has, I am afraid, beaten us. You have been extremely helpful and open with your answers. We are very grateful to you. I do not know if there are any final points which we have failed to ask you which you are burning to give to us.

(*Mr Burrow*) No, I think I have made the case and I will let it rest at that, but thank you.

Chairman] Thank you very much indeed and to Mr Black for coming to appear before us.

Memorandum by the Home Office including the Forensic Science Service

INTRODUCTION

This memorandum describes the Home Office responsibilities and interests in the use of digital images as evidence and gives a general overview of the issues, together with the civil liberties issues in the case of surveillance cameras.

11 December 1997]

[Continued

HOME OFFICE RESPONSIBILITIES/INTERESTS

2. The Home Office has responsibility for policy on the law on evidence in criminal proceedings; policy on the police enforcement of road traffic law, including the use of technology, the use of CCTV cameras in public open spaces and in prisons for security purposes; data protection legislation and the incorporation of the European Convention on Human Rights into United Kingdom law. In addition, Police Scientific Development Branch provides advice to both the Home Office and the Police on technical issues relating to law enforcement, including the use of digital technology and the Identification and Verification Services Directorate is responsible for managing the implementation of the new integrated services for fingerprint processing, which will use digital imaging. Also the UK Passport Agency and the Immigration and Nationality Directorate Department are developing programmes which involve the use of digital images in the context of their work, although these will not involve the use of such images as evidence to any great extent. The Forensic Science Service evidence is being submitted separately.

DOCUMENTARY EVIDENCE

3. Images produced on photographs, films, discs and video tapes can refer to pictures of a person or an object, either still or moving and also be documents. These can be adduced in evidence in criminal proceedings as a form of documentary evidence. As such, in addition to complying with the general rules on the admissibility of evidence, such images must meet two additional requirements relating to the proof of contents and proof of the fact that the document was properly executed.

4. In the case of proof of contents the courts have held that the document must be proved either by producing an original or a copy which has been proved to be authentic. However, there are exceptions both in common law and statute which provide for proof of documents by secondary evidence e.g. by a copy or a copy of a copy. In the case of tapes or films the courts have recognised that the rule about producing an original has no relevance [*Kajala v Noble* (1982) 75 Cr App R 149].

5. Proof of the contents of a document on which a party to criminal proceedings seeks to rely is largely governed by section 27 of the Criminal Justice Act 1988, which provides for the admission of a statement contained in a document (widely defined as meaning anything in which information of any description is recorded).

COMPUTER EVIDENCE

6. In addition where the evidence has been generated by a computer, section 69 of the Police and Criminal Evidence Act 1984 (PACE) requires a certificate or oral evidence to the effect that the computer was working correctly at the material time. The Law Commission, as part of its wider review on the law on hearsay evidence has recommended in its final report, which was published in June, that section 69 of PACE is repealed on the grounds that it serves no useful purpose. The Commission takes the view, which was supported on consultation, that section 69 fails to address the major causes of inaccuracy in computer evidence; advances in computer technology make it increasingly difficult to comply with section 69; the recipient of a computer produced document who wishes to tender it in evidence may be in no position to satisfy the court about the operation of the computer and section 69 does not apply in any event when such computer evidence is used by an expert in arriving at his conclusions. The Law Commission has concluded that it would be preferable to restore the common law presumption that, "in the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time." The Government is giving careful consideration to this proposal together with the others contained in the report.

DIGITAL IMAGES

7. In the case of the capture of live images (as opposed to digital technology used for processing and storing data from original documents), the main difference between digital images and conventional analogue images captured on film or video tape, both moving and still, is that there is no "original" image such as a negative or original tape but rather only a precursor image recorded electronically, which can be used to produce identical replicas. Also such images are stored as data on computer or a floppy disk and as such are the same as other types of data stored on computer.

8. All images, whether analogue or digital can be altered. Thus when determining whether to admit such images as documentary evidence, the court will need to be satisfied that the version of the image being presented to it has not been altered in any way and thus that it is either an original or an authentic copy. In the case of digital images, in the absence of an "original" image, authenticity can be established through the use of an audit trail which can be either procedural or electronic or a combination of both. Further details on this aspect are set out below in the detailed responses to the Committee's questions.

*11 December 1997]**[Continued]*

USE OF IMAGES IN CRIMINAL PROCEEDINGS

9. Images are presented in evidence in the courts for a wide variety of purposes, both in analogue or digital form or in a combination of both. Uses include traffic speed cameras, surveillance and fingerprinting. These uses and forecast future developments are also described in more detail below in response to the questions posed by the Committee.

CIVIL LIBERTIES ISSUES

10. The use of surveillance cameras, whether analogue or digital, does raise civil liberties issues, but controls already exist in those areas for which the Home Office has responsibility, for example, Part III of the Police Act 1997 provides a statutory base for police/customs surveillance operations. The Government has stated that it will consider the principle and practicality of underpinning existing codes of practice for public space CCTV systems into legislation. These issues are discussed more fully in the responses to questions 6 and 7.

September 1997

APPENDIX

HOME OFFICE RESPONSE TO QUESTIONS

QUESTION 1: (A) WHAT IS THE CURRENT AND FORECAST FUTURE USE OF DIGITAL TECHNOLOGY FOR IMAGE COLLECTION, STORAGE AND TRANSMISSION?

1.1 In the view of the Home Office this is increasing rapidly, although the rate of increase will vary across the many individual fields of use.

1.2 Some existing and imminent examples of the use of digital images are:

Still pictures

Prisoner photographs and witness albums.

Prisoner "live-scan" of fingerprints. These are both being used now and their use can be expected to increase steadily.

Police scenes-of-crime pictures including fingerprints. The use of digital still-picture cameras is being researched and standards for image quality and audit-trails are being developed by the Home Office.

General property photographs and antique indexes. These are being used now and their use may increase rapidly.

Surveillance photographs, particularly in relation to their immediate onward transmission over police radio/mobile telephone equipment. These systems are being used now, and their use may increase rapidly.

Road traffic accident records. Digital cameras are being used now and their use may increase rapidly.

Film scanners. For the digital storage of negatives on archiving systems such as Kodak Photo-CD and also storage of a photographic facial image. These are being used now and their use can be expected to increase steadily.

Fingerprint and mark images

The National Automated Fingerprint Identification System will go live in the summer of 1998. By 2000 it will store about 6 million ten-print records plus a similar number of mark images from scenes of crime, together with the associated textual information. All data will be in digital format. The data will be transmitted between the central site and the police force bureaux, and between bureaux, over the Police National Network. Many thousands of print and mark transactions will take place every day.

When NAFIS first goes live most of the image data will have been derived from conventional analogue sources such as ink-on-paper fingerprint forms and photographs and lifts of marks. However, it is expected that in the near future an increasing quantity of original data will be obtained digitally, using "livescan" ten-print capture units and digital cameras for mark capture. Thus there will be no original paper source to retrieve as "best evidence" in a court of law.

Immigration Correspondence

The Immigration and Nationality Directorate Casework Programme is in the process of designing and building a new computerised integrated case working system based on the electronic imaging of correspondence which will supersede the present paper-based methods. In many instances original

11 December 1997]

[Continued]

documents will be available to be produced in evidence in any court or tribunal proceedings but in some instances the only remaining evidence will be the electronic image.

Passport Photographs

The equipment to print the current passport is now obsolete and the photograph is vulnerable to photographic substitution. Therefore, passports are being upgraded in line with international developments. This will involve the digital capture, storage and transmission of the holder's image and signature for direct printing onto the passport after UK PA authorisation. Under this new system all records will be held on a computer data base, including the image and signature. The original paper record, which will include a photographic facial image and the applicant's signature, will be retained for a period of time, in case it is needed as evidence but will then be destroyed. After that in the fairly rare event that copy records are required for prosecution purposes the Agency would like to be able to rely on digitally imaged records rather than microfilm records which is the current practice. From 1999 the Agency expects to handle around 4 million digitally imaged passport applications each year and the ability to rely on digital copies would remove the need for costly storage and retrieval of paper records.

Video and TV Pictures

Video enhancement. Typified by the PSDB IMPROVE system which digitises images from analogue videotape under the control of an audit-trail. Although widely used, a more advanced system is under development. The use of similar systems and procedures is likely to increase steadily.

Digital video camcorders. Are used presently and their use is expected to increase very rapidly.

Digital video recorders, tape and disk-based. Are used presently and their use is expected to increase very rapidly. An example is the PSDB FULMAR system, in police use since 1995.

Digital TV transmission systems, both real-time and slow-scan. Are used presently and their use should increase steadily.

HM Prison Service uses CCTV extensively for security purposes. Images are recorded in some cases, and increasingly such recordings are made using digital techniques.

Access control and security systems. Used presently and their use is likely to increase rapidly.

Intelligent scene analysers based on neural networks. Are used presently and their use will increase steadily.

Vehicle number-plate readers. These are in use now and their use is expected to increase steadily.

Vehicle speed enforcement equipment permitted under the 1991 Road Traffic Act. These are likely to be in use within a year and their use will be fundamental to the efficient control of traffic flow.

1.3 Other common digital imaging applications are also in use such as facsimile machines and other transmission media.

(b) WHAT IS ITS USE BY THE COURTS AND THE LEGAL PROFESSION?

1.4 At present the use of digital image by the Courts is low but is likely to increase rapidly. In addition to the use for fingerprints and marks, vehicle number plate readers and vehicle speed enforcement mentioned above, some specific examples of the court use of digital images are:

- Since 1990, widespread use by the police of the Home Office IMPROVE image enhancement system. Its use as evidence remains unchallenged.
- Since 1996, digital images from the VIDEOVAULT system installed in the car parks at Heathrow Airport have been successfully used as evidence.
- The use of digital technology in the TV and video industry has been routine for many years, in signal conditioners such as Time-base correctors, also in Multiplexers and switching equipment. All video prints are also the result of digital processes.
- Since 1996, the Kodak Photo-CD system has been used to conveniently introduce large numbers of evidential images to a jury as an alternative to the high cost of producing multiple packs of photographs. A further advantage is that the court is certain that all members of the jury are examining the same picture at the same time. In this example the original negatives are retained, hence the legal issues are different than with all-digital systems.

1.5 Comments on the disadvantages of the use of digital still images compared with digital television and video are set out in Annex A.

*11 December 1997]**[Continued]*

(c) WHAT IS THE STATE OF THE ART OF IMAGE MANIPULATION?

1.6 The state of the art allows selective or global alteration to be made to any picture. Although still possible with specialised equipment, global alteration is presently more difficult with a succession of related images such as are required for television and video. Further comments on image manipulation are set out in Annex B.

QUESTION 2: DOES THE EASE OF COPYING, MANIPULATING AND TAMPERING WITH DIGITAL IMAGES, AND THE CONSEQUENT DIFFICULTIES IN MAINTAINING AN AUDIT TRAIL, MEAN THAT THEY SHOULD BE TREATED DIFFERENTLY WHEN USED AS EVIDENCE.

2.1 As indicated in the covering note, copying and manipulation can take place in respect of both analogue and digital images, therefore in the case of both types of image there is a need to satisfy the court as to its authenticity. Because of its nature, in comparison with photographic and analogue electronic images there will have to be some differences to the way in which digital images are brought to court, and the way they are considered. For example, as already indicated, the concept of an "original image" can not be applied to most still-picture digital cameras, and that of "copying" should be replaced with "replication". The "audit-trail" is then the essential link between a replication and its precursor.

2.2 Our view is that it is relatively easy to maintain an audit-trail for a digital image. We suggest there are two forms of audit-trail. The procedural form is where law-enforcement officers can testify that at every stage, named individuals have supervised the introduction into court of a particular image. It is then used to support other contemporaneous evidence they may present to illustrate a scene or incident.

2.3 An electronic audit trail is one where a file-code is introduced that relates to the data file representing the image. It must be capable of subsequent analysis to list all additional digital operations to that image, including enhancement or manipulation. The trail will therefore lead back to an image that has no other precursor. The security of this code may not be absolute, but should be generally acceptable without further proof of authenticity.

2.4 Audit trails, both procedural and electronic, form part of the systems being developed for the new National Automated Fingerprint Identified System. Audit trails are also being developed as part of the Immigration Casework System and the new Passport System. In the case of the Prison Service, the new generation of control room equipment will include facilities for any images which may be required as evidence to be copied immediately using CD-ROM or similar WORM technology and removed immediately from the equipment within a few minutes of the incident and immediately sealed in an evidence bag for storage.

QUESTION 3: (a) WOULD SPECIFIED MEASURES TO AUTHENTICATE DIGITAL IMAGES E.G. WATERMARKING, INCREASE THEIR UTILITY AS EVIDENCE?

(b) WHAT WOULD BE THE PREFERRED PRACTICAL MEASURE?

3.1 We believe the preferred measure would be a hybrid procedure using a procedural audit trail, followed at some stage by an electronic audit trail involving file-coding of the digital images. It is most likely that the electronic file-coding of digital images will occur at the time of down-load to a host computer. The recording medium should then provide a permanent physical record of the data which, once written, cannot be amended with new data. A procedural audit trail will then be required up to this point only. A "write-once, read many times" or WORM disc, is a recording device suitable for this application.

3.2 A watermark which we define as "embedded manipulation of a digital image to identify it uniquely, usually for copyright purposes", might be used as an adjunct to, and not a replacement for, the audit trail. For example, a water mark could be used as a key component of a procedural audit trail. However, the danger of using a "watermark", however this is defined, is that its introduction may itself cause an unwarranted and undetected alteration to the image. Furthermore, we believe that it is unlikely that any water mark will prove to be fully resistant to a determined attempt to undermine it.

3.3 In addition whilst an electronic image can be file-coded or 'watermarked' at the time of image capture, few cameras presently allow this. We take the view that this type of additional facility is unlikely to flourish in a mass-market, because of the additional equipment cost and of finding a specification acceptable to the foreign manufacturer of the digital camera. Even if this were possible, unaudited images would certainly find their way into court from the cameras of private individuals who possessed relevant evidence. The acceptability of these images will in each case have to be judged on merit. Our view is that most digital pictures of good quality will satisfy the court as genuine through a sensible analysis of context, viewpoint, perspective and lighting. To then oppose the validity of such a picture, some evidence of conspiracy will have to be shown.

*11 December 1997]**[Continued]***QUESTION 4: UNDER WHAT CIRCUMSTANCES AND WITH WHAT CONTROLS SHOULD MODIFIED OR ENHANCED IMAGES BE USED AS EVIDENCE?**

4.1 All images, both analogue and digital, can be thought of as “modified or enhanced” to some extent. Simple brightness or contrast changes, achieved using conventional photographic methods or by altering display parameters of a digital image, are strictly modifications to an image. The most severe form of image modification is arguably the initial capture using an analogue camera or digital scanner. The presentation of any image as an exhibit in court must depend on the circumstances and on the actual manipulation which has been applied.

4.2 Where, it is used in conjunction with a proper audit-trail, a modified image can aid the court process by revealing image information that was not visible before modification. Examples of this might be the use of image-processing algorithms for de-blurring or noise-reduction. The audit-trail should lead back to an unmodified precursor and a reasoned argument put forward to justify the choice of image processing algorithm for the specific image, or part of an image. This information should be fully documented and presented with the evidence. For example, the recommended procedures to be followed when carrying out announcements of fingerprint evidence are set out in “Code of Practice for Legal Admissibility of Information Stored on Electronic Document Management Systems”, BS1 1996.

QUESTION 5: DO TECHNOLOGIES WHICH COMPRESS DATA OR USE ERROR CORRECTION TECHNOLOGY WHEN TRANSMITTING IT RAISE SPECIAL PROBLEMS?

5.1. Data compression and error correction technology can cause problems not only when transmitting but also in other processes such as storage. A particular problem may arise with the MPEG (Moving Picture Expert Group) lossy compression system. In some situations this samples the incoming picture stream only periodically, and then by a prediction process recreates new intermediate pictures to provide a continuous output. Although lossy-compression may be suitable for some still-picture applications where its use has been fully assessed, only an existing system of “lossless compression” can be used without reservation in all imaging applications.

5.2. However, very rarely will the user have access to the uncompressed image. It should be appreciated that most digital cameras carry out some form of image compression in-camera to enable worthwhile numbers of images to be stored. This is a form of corruption of the image and it is essential that the image quality of digital camera systems are evaluated in relation to the particular application. Even those cameras which do not compress the data provided by the sensor will always modify it in some way with respect to the sampled values of grey-scale and chrominance.

5.3. In deciding whether image compression is, or is not, acceptable, the overall image quality requirement needs to be assessed against the imaging application. It is likely for example, that a system designed for digitising prisoners photographs will have very different requirements in terms of image quality, including data compression, to one designed for vehicle index plates. Some systems will need colour information, some will not. Regardless of the use of compression, there will always be some effect on grey-levels and colour balance. for these reasons the effects on images of any error-correction systems should be assessed in relation to the type of information which is being handled. At the present, our knowledge of these effects are incomplete and more work is required before we are in a position to understand them.

5.4. When an image is being transmitted, full error checking is essential. We wish to draw attention to the Home Office and ACPO guidance given in PSDB report 3/96, Specifications for Automatic Traffic Enforcement Systems, by Dr S Lewis. This also requires standard message authentication codes, as used in the banking industry, to be appended to the image prior to recording and transmission. By following this guidance and recording immediately on to a WORM, the concept of an “original image” is closely maintained.

5.5. It should be noted that under section 20 of the Road Traffic Offenders Act 1988 (as amended) provision exists for the type approval of devices which produce a record or measurement as evidence of an offence. Such a requirement has been made in respect of speed and traffic light enforcement cameras. Within the well-established approval process devices are tested to standards published by PSDB. The process provides a public assurance of a device’s accuracy and reliability and the scientists at PSDB will be supporting us in ensuring that only those digital devices meeting their standards for obtaining and then safeguarding evidence will be put forward for type approval.

QUESTION 6: DO SURVEILLANCE CAMERAS, PARTICULARLY IF USED IN CONJUNCTION WITH IMAGE TRACKING SOFTWARE, THREATEN CIVIL LIBERTIES?

6.1. Any use of surveillance cameras has implications for civil liberties. This is true whether they are analogue or digital, and whatever software techniques are employed to process the information they capture. A balance needs to be struck between the operational benefits such cameras afford and their effects on public

11 December 1997]

[Continued]

liberty. To safeguard the public, the operators of such camera systems need to have in place sufficient management and control mechanisms to ensure that the systems are only used in the public interest.

6.2. Surveillance systems operated by the police have such mechanisms in place (see question 7 below). But there are other surveillance cameras, both public and private, operating throughout the country. These range from large public space closed circuit television (CCTV) schemes to single camera corner-shop systems. In general, they are analogue systems—cameras relaying images to monitoring screens backed up by videotape machines. But as the technology develops it will be possible to upgrade the equipment to include digital elements or to full digital operation.

6.3. Most public space CCTV systems are owned and operated by publicly accountable bodies such as local authorities. Such bodies have an interest in retaining public support for their CCTV schemes. They will, consequently, ensure that they have well-developed codes of practice in place which specify, among other things, how the information obtained is handled. Every CCTV scheme receiving Home Office funding is required as a condition of grant to have in place such a code of practice. The Home Office has no information on the use of codes of practice by operators of private CCTV schemes.

QUESTION 7: SHOULD THERE BE STATUTORY CONTROLS ON THE PLACEMENT AND USE OF SURVEILLANCE CAMERAS AND RELEASE OF INFORMATION FROM THEM?

7.1. When considering the issue of controls on the surveillance cameras, the United Kingdom must have regard to the European Convention on Human Rights (ECHR) and the UN International Covenant on Civil and Political Rights (ICCPR).

7.2. Article 8 of the ECHR states:

- "1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
- 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

7.3 Article 17 of the ICCPR provides:

- "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation.*
- 2. Everyone has the right to the protection of the law against such interference or attacks."*

7.4 UK law does not include a general right to privacy, but contains a number of statutory provisions to safeguard privacy which apply in particular circumstances, such as criminal or civil trespass, contract, copyright or breach of confidence. These laws provide the safeguards necessary for compliance with our international obligations. The government is currently preparing proposals for incorporation of the ECHR into domestic law. Following incorporation, it will be for the courts to interpret Article 8 in the context of UK law.

7.5 Controls (statutory or otherwise) already exist in the areas for which the Home Office has responsibility. They are as follows:

A. Police use of surveillance cameras

Home Office guidelines issued in 1984 advise the police on the use of surveillance equipment. Paragraph 16 makes it clear that the use of surveillance equipment *in a public place* should be authorised by a Chief Superintendent. The officer should first satisfy himself that the use of the equipment will not involve unwarrantable intrusion of privacy and is fully justified in all the circumstances of the temporary or standing police operation in question.

Where visual surveillance takes place *in a private place but with the consent of a person who is party to the events being observed/recorded*, authority may be given by an Assistant Chief Constable. Where the surveillance takes place *in a private place where there is no consent*, authority rests with the chief officer.

The use of intrusive surveillance by the police and customs involving entry on and interference with private property where there is no consent was made the subject of statutory provisions in sections 92 to 108 of the Police Act 1997. This sets out the procedures for authorisations by chief officers and for oversight by Commissioners (serving or former High Court Judges). Those deploying intrusive surveillance techniques will be required to comply with a code of practice which is currently the subject of a public consultation exercise.

Information obtained by means of intrusive surveillance will be admissible in court. However, Commissioners will have the power to order the destruction of records in cases where they quash or cancel an authorisation, other than those records required for pending civil or criminal proceedings. They will also be responsible for investigating complaints.

11 December 1997]

[Continued

Work on implementing the provisions is underway with a view to them being brought into force early next year.

B. Automatic traffic enforcement cameras

Where automatic speed and traffic light cameras are used to detect offences drivers are traced via vehicle registration records and this will remain the procedure when these cameras are updated to use digitised images. The security of images is addressed during type approval testing. In response to concerns about car user privacy advice to the police has highlighted the need for circumspection in dealing with photographic records. Most recently, ACPO's Traffic Committee has issued advice to forces about the use of front of vehicle photography for speeding offenders.

C. Public space CCTV schemes

The Home Office has assisted in funding around 550 CCTV schemes over three challenge competitions. More than £37 million has been distributed since 1995. One of the primary eligibility criteria is the existence of a suitable code of practice for the scheme. Such a code should cover as a minimum requirement:

- operator selection and training;
- control room procedures (logs, records, manuals, etc.);
- tape management (re-use, storage, care of evidence, etc.);
- tape access (who has access, under what circumstances, authorisation procedures for release, etc.);
- accountability (lines of command, etc); and
- checks and controls (standard procedures, performance checks, etc.)

No system received funds unless such a code was in place.

The government has endorsed the publication by the Local Government Information Unit (LGIU) of a model code of practice for CCTV systems—"CCTV—A Watching Brief". Although it recognises that codes of practice inevitably differ according to the type of system and the area covered, and that only local system operators will know what is the most appropriate regime in their particular circumstances, it also sees the LGIU's model code as a useful contribution to the debate, and a helpful guide for those drafting codes of practice.

D. Data protection legislation

Some surveillance processes may fall within the scope of current legislation—the Data Protection Act 1984, Home Office advice to CCTV operators is to conduct their business as if the legislation does apply, since this is simply good practice. The Government will shortly be bringing forward a Data Protection Bill to give effect to the EC Data Protection Directive. This applies to sound and image data relating to individuals which are processed in the course of activities which come within the scope of EC Law. The main thrust of the Bill will be to apply the Directive's regime to all processing of personal data whether or not the activities in question are within the scope of EC law.

7.6 Despite this regime of general and specific measures, the government recognises that there are concerns about accountability and control, particularly of CCTV schemes, both public and private. Individually developed codes of practice can lead to a lack of consistency and not all schemes are obliged to adopt them. The government has therefore stated that it will consider the principle and practicability of underpinning the existing codes of practice with legislation.

QUESTION 8: SHOULD FURTHER ADVICE OR TRAINING BE PROVIDED TO LAW ENFORCEMENT OFFICERS, AND THE COURTS ON THE TECHNICAL LIMITATIONS OF THIS TECHNOLOGY?

As indicated in response to earlier questions some advice has already been issued. Further advice (including training) may be necessary but we have not yet assessed the issue fully, nor decided what form any advice might take and how best to disseminate it. We would also like to take account of the Committee's views once it has studied all the evidence on the risks and limitations of the technology.

*11 December 1997]**[Continued]***QUESTION 9: IS THERE THE NEED FOR SPECIAL MEASURES TO CONTROL THE PUBLICATION OF MODIFIED IMAGES BY THE MEDIA?**

No comment. The policy responsibility lies with the Department of Culture, Media and Sport.

Annex A**COMPARISON OF THE USE OF PHOTOGRAPHIC AND STILL DIGITAL IMAGES**

1. In many applications, the use of digital still-picture cameras can be less appropriate than conventional photographic cameras. If for example a CCD sensor typical of present design is to have an image-quality similar to that of a medium-speed photographic film, its area will be approximately 10 times larger than the film format. The use of a larger CCD with proportionately more pixels to match the quality of the photographic film, will then demand an unusually large storage capacity, lengthening the transfer time to the storage medium and limiting the rapidity with which successive pictures can be taken. Such large CCDs presently cost several thousands of pounds and take a minimum of several seconds to download. The nature of the image produced by a digital camera is also very different to that of a conventional photograph. Images recorded on film are [isotropic], as is the real world, whilst that from a CCD is not and often introduces unwanted image artefacts due to aliasing. Film offers considerable flexibility in terms of exposure adjustment whereas most CCDs can not accept long exposures without introducing electronic noise to the image.

2. For these and other reasons, the suitability of digital still-picture cameras should be carefully considered in relation to the specific application. Typical factors to be assessed are the image quality, sensitivity, storage capacity, transfer time of images, also the total cost of the camera and associated equipment for the display, storage, retrieval and reproduction of the images. We expect the use of conventional photographic technology and equipment to remain predominant among the police and the general public for many years.

COMPARISON BETWEEN ANALOGUE AND DIGITAL TELEVISION OR VIDEO

3. The case of digital television and video is however very different, as the image quality advantages over analogue systems are overwhelming and there is no loss of image quality across many generations of replication. Digital television camera equipment has been used by the media in this country for over a year and is replacing analogue equipment and systems very rapidly. In many television studios the input signals, their switching, conditioning, editing, recording and re-transmission are completely digital. In the CCTV security industry there are now great pressures from manufacturers towards the use of digital recording equipment. A complete range of domestic and low-end professional digital video equipment is newly available, and will be widely used by the police because of its image quality and the ability to obtain any number of perfect reproductions.

Annex B**MANIPULATION OF DIGITAL IMAGES**

1. The range of manipulative operations that can be carried out on a digitised image is virtually unlimited. Examples of accepted practice are the adjustment of tone and contrast or the integration of a number of related moving pictures. Nevertheless, some forms of this simple "enhancement" are potentially dangerous and could intentionally or accidentally produce misleading images, fourier filtering is one example of this, unless used in certain controlled circumstances. The enhancing of compressed images may also lead to visible artefacts which in some circumstances could be misleading. Other operations should be specifically prohibited. Some examples are those that involve individual pixel manipulation such as introducing details from other images, the use of "air-brush" programs for changes to local or global colouration, and "morphing" where two or more pictures are seamlessly distorted or merged.

2. It would be convenient to find a clear definition of an "enhanced" and a "manipulated" image. This would allow an "enhancement" to be viewed as an improvement to the original picture quality without loss, addition, or alteration of picture content. In this case the processes of improvement would usually relate to accepted photographic process where global adjustments are made to picture tone, contrast, black and white levels, also edge detail. They also relate to the familiar adjustments found on domestic television receivers. Such changes to the image would then normally be accepted by the court. A "manipulated image" would on the other hand be one in which a material alteration of picture content is involved, whether inadvertent or malicious. In both cases there must always be a precursor image that can be related to the enhanced or manipulated replication. A proper "audit-trail" will show the relationship between them.

3. However, it may not be easy, or even possible, to define the point at which an enhancement of existing information becomes a corruption. Therefore, although an audit-trail is always essential, if a particular "enhancement" algorithm has been applied locally or globally to an image, it must also be accompanied by a reasoned justification of its use.

*11 December 1997]**[Continued*

Evidence from the Forensic Science Service

1. INTRODUCTION

1.1 Digital images are two-dimensional electronic representations of three-dimensional space. They are stored as digital data on computer media and, as such, they are no different from any other type of data stored on computer media. They should thus be subject to the same considerations as other computer data in respect of their security, integrity and handling within the criminal justice system.

1.2 Within the FSS, digital images are processed and examined in a similar way to all other evidential materials, according to written policies and procedures within our Quality Management System and using validated techniques. The policies and procedures have been written to take full account of the requirements of the criminal justice system and have been externally accredited by third parties as being compliant with the NAMAS M10 (ISO Guid 25) and ISO 9000 series of standards¹.

1.3 An overview of the "forensic process" for digital images is attached. We discuss below those aspects of the process which we feel it is important to consider as potential points of concern for the criminal justice system.

2. THE FORENSIC PROCESS FOR DIGITAL IMAGES

2.1 *Seizure of items containing digital data*

It is always possible that any item containing digital data could be mishandled or deliberately tampered with, and the data subjected to some sort of processing, during seizure of the item by the investigating authority. The integrity of the data can also be compromised by the subsequent inadequate handling, packaging and storage of the items seized, for instance by exposure of the items to magnetic fields. Such activities should therefore be carried out only by competent persons following validated protocols.

2.2 *Transfer/transportation of items containing digital data*

Once seized, the data needs to be made available for examination. Modern communication systems make it unnecessary for evidential material already in digital form to be physically transported to the laboratory. It can also be transferred, for example, by telephone and over computer networks. Physical transport requires the same considerations as apply to storage of the items. Where electronic transfer is chosen, it should be adequately tested and controlled in order to ensure system integrity.

2.3 *Capture of images as digital data*

There can be no control by the investigator or laboratory over the capture of images which are in the form of digital data when seized, although where necessary the image capture system can be checked to ensure that it is functioning correctly. Image capture systems in use by investigators or the laboratory, however, must be validated for the purpose for which they are to be used. This requires a clear and full understanding of the image capture process, particularly of its limitations and the possible effects of these on data. The integrity of the system must also be maintained thereafter on all occasions it is used and this must be capable of demonstration. And there is the issue of the competence of the operator, who should be properly trained, in possession of relevant qualifications, working to documented procedures and subject to a quality assurance regime. At all times the requirements for continuity must be observed.

2.4 *Preservation and copying of digital data*

Copies of the original digital data should be made as soon as possible after receipt of the material by the laboratory and all work should be carried out on the copies so as not to risk corruption of the original. If more than one copy is required for this purpose, then the replicates should also be obtained direct from the original to provide best evidence. Arrangements must be in place for the secure, tamper-proof storage of the original items and digital data. This requires consideration of such factors as the storage medium involved, environmental conditions, auditing and the possible need for access to the data at a much later date (eg for appeals) when current systems may no longer be compatible.

¹ "The FSS manages the handling of evidential materials and scientific processes according to written policies and procedures and uses validated techniques. The quality management system which controls these activities is assessed by the third party organisations UKAS and BSI.QA. Most of the technical procedures have been assessed as part of the accreditation process. The FSS image processing procedures themselves have not yet been assessed by UKAS or BSI.QA. The FSS intends that this work will be assessed and added to the scope of accreditation in due course and will take into account the results of our research."

*11 December 1997]**[Continued]*

2.5 Forensic examination

All methods used for the examination of evidential material must be fully validated as fit for purpose. Methods for digital processing should be shown to be robust and reliable, to give results in accord with expected outcomes, to be fully documented and to be generally accepted by the scientific community. There should be appropriate arrangements in place for the calibration and maintenance of any equipment used and for quality assurance. The users of the methods should possess a full and clear understanding of digital processing and should be capable of demonstrating their competence in the work.

2.6 Provision of corroborative evidence

The main purpose of forensic examinations is usually to provide corroborative evidence of identification or comparison, or to help interpret information, the overall result being expressed as an expert opinion. It is just as important to control this aspect of the work through standards and protocols as the experimental work. The opinion should be soundly based and take into account any issues arising from the circumstances of evidence seizure and any limitations in the method employed that were revealed by the validation process. The qualifications and competence requirements for the person giving the expert opinion are also of paramount concern. Interrogation of reference computer databases containing images (eg a collection of fingerprints or footwear impressions) can be a standard procedure and use of these databases must also be regulated and validated.

2.7 Provision of intelligence information

Digital data may be used for intelligence purposes as well, but the same standards as for corroboration need to be ensured, since in some instances the data could ultimately be called as evidence in court.

2.8 Court presentation

Experts called to give opinions on evidence from digital data need to demonstrate to the court's satisfaction they are qualified to do so. The experts' primary duty is to the court and it is thus incumbent on them to bring to the court's attention any potential pitfalls associated with the presentation of such evidence. With the advent of video clips, multimedia and virtual reality, it is essential that the courts are advised of their limitations and the potential prejudicial possibilities of such techniques.

3. RESPONSES TO SPECIFIC QUESTIONS

3.1 What is the current and forecast future use of digital technology for image collection, storage and transmission? What is its use by the courts and the legal profession? What is the state of the art of image manipulation?

3.1.1. Digital image capture is used in the FSS for a variety of purposes, ranging from recording of notebooks to images of physical evidence. Where digital imaging offers a commercial and/or technical advantage over existing methods it will continue to be chosen as the preferred option when upgrading technology or developing new forensic techniques for image collection, storage and transmission. Once an image is in a digital form the data can be stored on a variety of media and the FSS uses a number of these, including hard drives, optical discs and CD-ROMs. The transmission of digital images over public networks such as the Internet or digital telephones is not currently carried out by the FSS, although, as a multi-site organisation, it is anticipated that internal network systems for remote access to central databases will soon become available, and digital images will almost certainly feature as a part of these (eg the footwear database). In the future, scene of incident to laboratory communication systems may also be another area for image transmission.

3.1.2 Digital images are mainly used in court by the FSS as part of hard copy case notes in the same manner as Polaroid photographs. Digital images submitted to the FSS as exhibits are also usually presented to the courts in a hard copy format. However, in the future, with the increased availability of computer technology within courtrooms, it will be possible to show the images directly on screen. Video recordings are already used in certain cases, but new digital media may soon be available to the courts allowing, for example, scene reconstruction and scenario testing, and use of three-dimensional CAD images, digital video clips, and virtual reality as presentation tools.

3.1.3 Digital image processing is an active research area and new techniques are evolving continuously. The FSS is not a centre for research in digital image processing and therefore does not feel that it can comment further on state-of-the-art image manipulation.

11 December 1997]

[Continued

3.2 *Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean they should be treated differently when used as evidence?*

3.2.1 We do not feel that digital images produced as part of the forensic examination of an exhibit require any special consideration for use in the criminal justice system. The production of such images is controlled through our Quality Management System and subject to third-party accreditation in the same way as any other forensic technique. The maintenance of an electronic audit trail in these circumstances is possible, but in our view what is more important are adequate records to allow a competent person to repeat the operation.

3.2.2 Where digital images are submitted to the FSS as evidential exhibits there is always the possibility that they may have been processed digitally in some way before coming into the possession of a law enforcement officer. However, the integrity of all evidence types is subject to the possibility of undetectable compromise before we receive them and this has to be taken into consideration when formulating an opinion based on the evidence found. So, again, we do not see digital images as requiring any special treatment within the forensic process.

3.3 *Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence? What would be the preferred practical measure?*

3.3.1 The use of measures to demonstrate faithful reproduction of images (digital or otherwise) is not seen as essential for images produced and used only within the confines of the FSS as part of a case examination. The reproduction process will be adequately covered by the Quality Management System and will have been demonstrated to be fit for purpose.

3.3.2 Digital images which are to be used for evidential purposes and are transmitted over public networks, however, should have a level of security that ensures that they cannot be altered during the process, for example by a third party intercepting the image at some point or the method of transmission itself altering the original data. To reduce the risk of third party interference some means such as encryption could be used. Encryption is not infallible, but it can act as a powerful deterrent. Other technological solutions to authentication are equally likely to have limitations. They will ultimately be circumvented by ingenious and determined wrongdoers, and higher security means higher costs. It is probably better to assess the risks of digital data corruption during the process of transmission as part of the validation of the process and to monitor the integrity of any transmission system operationally by the use of controls.

3.4 *Under what circumstances and with what controls should modified or enhanced images be used as evidence?*

3.4.1 The enhancement of images is not a new process. For example, photographers have long improved the subjective quality of their images by adjustment of contrast by varying exposure times. Digital techniques for the enhancement of images can be used for similar subjective purposes. If the adjustments do not result in the loss of detail in the image of direct evidential importance, or create new detail not present originally, then it is in our opinion of no consequence.

3.4.2 There is a danger, however, where digital image processing is used evidentially for comparison purposes, of making images, either deliberately or unintentionally, look similar when in fact they are different. The proper validation of such corroboration methods is thus essential. It is also possible with modern sophisticated electronic equipment for analogue image enhancement to incorporate digital processing techniques, and sometimes this can happen without the operator being aware. Such "black box" type systems need to be thoroughly understood and also carefully validated before being used in operational forensic case examinations.

3.5 *Do technologies which compress data or use error correction technology when transmitting it raise special questions?*

3.5.1 Compression techniques which do not allow recovery of the original data are not used by the FSS on digital images captured for evidential purposes. Compression techniques reduce the quality of the original image and we would consider it a regressive step to process this image rather than the uncompressed image. Compression techniques are not seen as a problem for digital images created within the FSS for non-evidential purposes.

3.6 *Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?*

No comment.

11 December 1997]

[Continued

3.7 Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?

No comment.

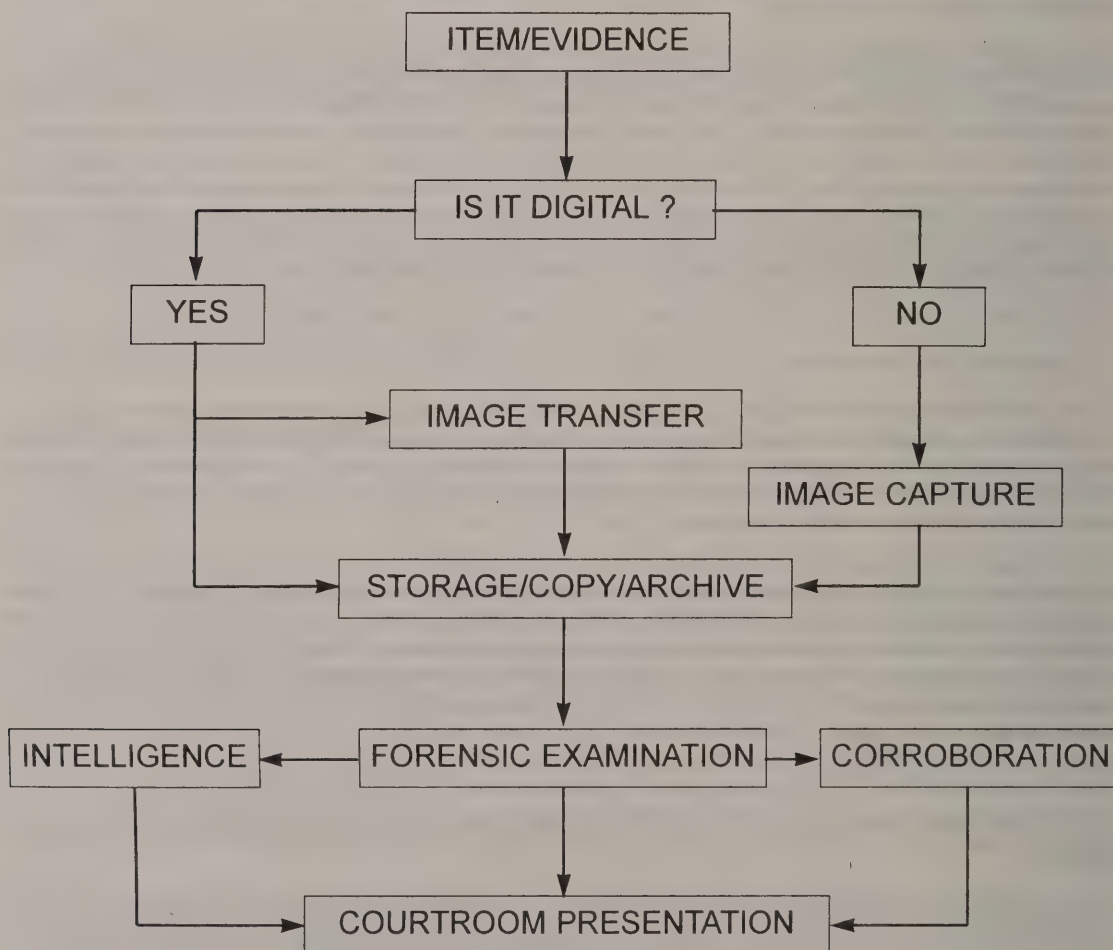
3.8 Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?

3.8.1 Imaging technology is evolving rapidly and it is important that law enforcement officers and the courts are kept fully apprised of its potential and limitations. Training should include awareness of how such images are used in forensic examinations and the information required from police officers and scene of crime officers when submitting such material for examination. The technical limitations of the technology and the potential pitfalls if procedures are not followed to prevent the corruption of the information either intentionally or accidentally should also be emphasised. The FSS provides such awareness training for other types of evidential material and could readily extend this as required.

3.9 Is there the need for special measures to control the publication of modified images by the media?

No comment.

THE FORENSIC PROCESS FOR DIGITAL IMAGES



11 December 1997] DR ROBERT BRAMLEY, MR RICHARD CHILDS,
MR SIMON HICKSON, MR PAUL PUGH, MS BRENDA HAWKYARD, [Continued]
MR JIM ALDRIDGE, AND MR ROY THOMPSON

Examination of Witnesses

DR ROBERT BRAMLEY, Chief Scientist, Forensic Science Service, MR RICHARD CHILDS, Head of Crime Prevention Agency (public space CCTV), MR SIMON HICKSON, Head of LGDP Unit (data protection and data matching issues) MR PAUL PUGH, Head of OPPU (police use of CCTV for road traffic control and regulation of the private security industry), MS BRENDA HAWKYARD, POCU (police surveillance issues), MR JIM ALDRIDGE, Police Scientific Development Branch (technical aspects of digital images and CCTV), and MR ROY THOMPSON, Police Scientific Development Branch (technical aspects of digital images and CCTV) the Home Office, called in and examined.

Chairman

423. Ms Hawkyard and gentlemen, good morning. Thank you very much for coming. You have come in some force and I recognise that this reflects very much the wide and disparate areas within the Home Office covering the areas of the topic in which we are particularly interested. I am not quite sure whether I address my questions collectively or whether one of you would like to be the leader. The latter would be helpful from our point of view and obviously you can ask your colleagues then to speak as necessary.

(Mr Childs) I think I have the dubious task of attempting to speak initially for the group.

424. Fine, Mr Childs, and thank you very much for that. Have you any opening comments before we start?

(Mr Childs) Yes, I have a few opening broad comments. As you said, my Lord Chairman, in your introduction, the reason why there are so many of us here is because this is a complex issue which impinges upon a number of areas within the Home Office, but the Committee's enquiry as a whole touches on some central issues which have a bearing on different responsibilities. These include the policy on the law of evidence in criminal proceedings, the policy on police enforcement of road traffic law, including the use of technologies, the use of CCTV cameras in public open spaces and in prisons for security purposes, data protection legislation and the incorporation of the European Convention on Human Rights. I myself am Head of the Crime Prevention Agency which deals with CCTV in public places, including the CCTV competitions. The Forensic Science Service provides scientific advice in the support of the investigation of crime and expert evidence to the courts. The Police Scientific Development Branch provide advice to both the Home Office and the police on technical matters relating to law enforcement, including the use of digital technology, and the Identification and Verification Services Directorate is responsible for managing the implementation of the new integrated services for finger-print processing which will use digital images. The Home Office has submitted detailed evidence and this was fairly technical in nature merely because it had to be to deal with the issues that were raised and I would point out that, speaking for myself, I am not a technical expert on these matters. There are some technical experts here whom we can always come back to if it gets too difficult. The key points in those submissions, my Lord, if I might just remind the Committee of those, was that all images, whether analogue or digital, can be altered. Therefore, when considering evidence in the form of an image, courts need to be satisfied that the version of the image produced to it has not been

altered in any way and, thus, that it is either an original or an authentic copy. In the case of digital images, in the absence of an original image, authenticity can be established through the use of an audit trail which can either be procedurally introduced or electronically done or a combination of both. Finally, CCTV cameras, whether digital or analogue, are used for surveillance in a variety of different contexts and the Home Office accepts that this raises civil liberty issues, but there in fact are already guidelines in existence for the police and for customs use of these technologies and the Government has endorsed the publication of the Local Government Information Unit's model code of practice for the use of public space CCTV. I hope, my Lord, that is a helpful overview of where we are coming from.

425. Thank you and I of course make the point that your written submission has been very helpful to the Committee. Starting off with the Local Government Information Unit's code, which seems to be very sensible, but it is, we understand, voluntary and applies only to the public sector, would you like to give us any feel for how the Home Office sees future developments with such a code? Should it remain voluntary or should it be enhanced by some statutory regime?

(Mr Childs) The Government is looking at the whole issue of regulation of private security and it could well be that in its deliberations, which are not complete yet, it chooses to consider some sort of regulation of this particular issue. The difficulty is that there are many systems in many contexts and it would be very difficult to produce one set of guidance which would actually cover all uses, and indeed I suspect there would be an issue of enforcement and making sure it happened out of the public sector. However, this is a matter upon which the Government has yet to finalise its position, but the indications are that it is certainly giving it some thought.

426. So clearly there is a perception then within the Home Office and the Government that this is an area which needs to be looked at further?

(Mr Childs) Yes, I think that is fair.

427. This is of course helpful in what it indicates, but taking that just a bit further, have you got any indication as to how soon this review might be completed?

(Mr Childs) I think that will probably get tied up with the timetable for legislation which looks to be rather more medium than short term, I think. That does not necessarily imply that there is not a will to do something about it, but I think it is a question of

11 December 1997] DR ROBERT BRAMLEY, MR RICHARD CHILDS,
MR SIMON HICKSON, MR PAUL PUGH, MS BRENDA HAWKYARD,
MR JIM ALDRIDGE, AND MR ROY THOMPSON

[Continued

Chairman *contd.*]

trying to monitor all the timings on these things, so I cannot be specific as to when.

Lord Brain

428. Is it likely in any way to be linked, from the evidence we have just heard, with the revision of the Data Protection Act or anything like that or are they two completely different trails?

(*Mr Childs*) I do not know if one of my colleagues could help me on that.

(*Mr Hickson*) Perhaps I can comment on the data protection side. We are in any case going to revise the Data Protection Act in line with the EC Directive. We would expect any guidance or codes which were issued on digital imaging or CCTV to take account of the prevailing data protection law. So they are really tangential issues.

Baroness Hogg

429. I think this is for Mr Childs again following up and going on from the point we have got to. Given that this is under review, however, could you share any thoughts with us at this point about the difficult issue of the distinction between the public sector and public space areas which the public has access to because it is not very easy for the public always to tell whether it is in an area owned by the local authority or privately owned for the purposes of shopping malls or indeed what the relevant criterion is, whether it is ownership, leasing, operation or whatever?

(*Mr Childs*) I do not think I can give a particularly helpful answer because this is a problem that goes way beyond just the issue of digital images and there is always going to be some confusion about when something becomes private and something becomes public, so I do not think I can be very helpful. I think the point that perhaps needs to be made is that if you come from the other direction and ask what are we trying to achieve, which is some sort of code of practice or some standards or some protections, then if it is decided that it is going to happen, then the private property issue will have to be specifically addressed and it can be legislation, but whether that actually follows through to what happens in practice is very difficult. A law could be passed, but the reality of enforcing it on private property is very difficult and indeed there is nothing to stop private people surveying public property, so I am sorry I cannot be more helpful than that because it is a very difficult area.

430. But perhaps one of your colleagues could just take it a little further in regards to present practice because, as you say, this does not just apply to the issue of digital images, but to all forms of surveillance, so what is the present practice?

(*Mr Childs*) I think the present practice is that on the schemes that have come from government initiatives, the CCTV schemes, there is, by definition, an acceptance of guidelines in the use of those schemes. The police and customs, as I have said, are covered by guidelines as to when and where they can use them in authority levels. As regards the use of this kind of technology on private property, there is, as

far as I am aware, no specific regulation at all. Therefore, that, I think, represents the present situation and any change then buffers up against the issues that I raised before. I do not know if any of my colleagues can add to that. Seemingly not. I think that is about as far as I can take it, but I think the more important issue in a sense is how do you make people on private property comply with any regulation you put in place if they do not want to.

431. That is the parallel issue of awareness of whether you are on public property and the regulation.

(*Mr Childs*) Indeed.

Lord Howie of Troon

432. There is a little shop which sells electronic equipment of various sorts not far from St James's Park tube station which has a camera pointing out into the street so that as you look into the window, you can see yourself on a screen. Is that an invasion of a public space by a private enterpriser?

(*Mr Childs*) Legally, I think not at the moment. Indeed Dixons frequently have shops doing exactly the same thing. It is a method of selling things, I think.

433. Not to me!

(*Mr Childs*) I think it would go to the issue about whether you attempted to regulate how you would actually stop that, but at the moment it is not an issue.

434. Would you like that to be stopped?

(*Mr Childs*) I do not think I can comment as to whether I would like it or not. I think that would be a matter for ministers who would wish to make a judgment on it.

435. You could probably tell them something, could you not? Do you not ever advise ministers on some things?

(*Mr Childs*) At the moment I think I am not supposed to say what I advise them. That may well change.

436. If you say, they will listen.

(*Mr Hickson*) Perhaps I could comment from the point of view of general policy on privacy. We can all look at each other in the street and photograph each other on a beach, so just looking through a camera is hardly a serious invasion of privacy. What would matter is any use made of information "back of camera".

Lord Nathan

437. My Lord Chairman, my question has to some extent been answered. What I was concerned about, and perhaps our witnesses might feel unable to answer it, but reference has been made to the problems and the questions of control and regulation and so forth. What I think I would like to know is how do you see the problem that you are trying to confront and, therefore, to what would the regulations be directed, so going no further than that, but if you cannot tell us what you see as the problem, we are left a bit adrift, I think.

11 December 1997] DR ROBERT BRAMLEY, MR RICHARD CHILDS,
MR SIMON HICKSON, MR PAUL PUGH, MS BRENDA HAWKYARD,
MR JIM ALDRIDGE, AND MR ROY THOMPSON

[Continued]

Lord Nathan *contd.*]

(*Mr Pugh*) I can speak from the perspective of ministers' views in relation to the private security industry which I think is one of the areas that you are looking at. I think it stems originally from a concern that people often put their trust in those that they employ to exercise certain functions, whether it is guards or door supervisors or other people working in that area, so I think ministers' prime concern is, in a sense, to protect the public, to ensure that those who are offering services to the public where they may be in a position either to put people or property at risk, that unsuitable people are not, as it were, permitted to set themselves up and offer those range of services, so that anyone who actually purchases some form of private security service has a degree of confidence that the person they are buying it from is not a crook and has some degree of confidence in the standard of service that they can expect to receive. So it is partly a question of probity as well as a question of standards of service and it is from that perspective that ministers are approaching the issue of the regulation of private security.

438. Yes, that is private security and I quite follow that, but talking of the subject we are concerned with of CCTV, which may be beyond what you have so far considered, I think many people feel that there is not undue concern with regard to CCTV under the control of the police and it may be that there would be regulation and so forth, but it is very extensively used in the private sector for the protection, as it is put, of the property of the person using it and some concern has been expressed as to the regulation of that use by the owner of the shop or whatever it is. Have you any view on that, whether there are any regulations required and, if so, to what they should be directed?

(*Mr Childs*) I think at the moment it is not possible to say what the view of ministers towards that very specific issue would be. I do not think it is one which, to be frank, has exercised their minds, certainly not to my knowledge. That does not mean it has not exercised their minds, but not to my knowledge.

(*Mr Hickson*) Perhaps I can comment from a slightly different angle, looking not at CCTV cameras in particular, but at information about people. The Government is due to introduce a Bill before Parliament in this session to extend the present data protection law. Now, I cannot at this stage go into the detail of what the Bill will say, that would be for ministers, but it would impact much more directly than present law on systems which process personal data, including pictures of identifiable people. What happens at the "back of camera" is likely to be caught by the general framework of data protection law in future. It will be enforced by the Data Protection Supervisory Authority, and apply to systems operating in the private and public sectors. So this general framework of law is likely to become increasingly relevant to CCTV.

Lord Brain

439. I am going to deal with two, so to speak, consecutive questions about the processing of images, handling of images and things like that.

There is a general perception, and I think probably justified, that undetectable modifications of an image, be it a digital image or even an original, what I would call, traditional photographic image, using digital technology can be made almost undetectably, and the general perception is that if you get presented with a thing that looks like a photograph, it is a photograph, even though in the old days it could have still been modified in certain ways without too much difficulty. How much authentication is required when a photograph is produced in evidence? Do you think that there should be codes of practice, as we were discussing earlier? What about audit trails and things like that? Can you give a general overview of presentation of images? I refer here not only to moving images, but also still images for forensic purposes.

(*Mr Aldridge*) This is a very complicated process and I do not want to get too deeply into the techniques and technology of it.

440. No, it is more the policy I am looking at really.

(*Mr Aldridge*) I think that the way we have handled visual images in the past, where they have been on video tape, has been quite easy because they tend to be continuous streams of images and, therefore, it is relatively easy to see if there is some discontinuity showing that some change has taken place. If it was necessary to do it, and thankfully it has only been on a few occasions, to check to see whether a tape has actually been tampered with, it is possible to do that. It is a very painstaking and exhaustive process and, therefore, it is not one which we wish to publicise. With digital images, you have a totally different problem and I think that it is relatively straightforward, now that principles of practice and standards exist, to apply a suitable code to a digital image which ensures that subsequently, if someone looks at that image and checks the code, they can see that the image is the same as the one they started off with and that it has not been tampered with. One of the prime problems is applying that code at the point of origination of the image. If you apply it later, then you have to have maintained sufficient control to ensure the integrity up until the point where you apply the code. If you are going to transmit the image for instance, you would have possibly to think about encrypting the whole process and again all of those processes are very clear. Standards exist especially for single images. There is an important issue here which I think people need to be clear about and it does worry me slightly. Current technology enables you to do this for single still images very, very easily, it all exists and it is done. TV cameras produce five million pictures a day and to encode the whole of that stream effectively using this kind of process is still quite expensive and, therefore, if you were to try to introduce that approach generally to CCTV, rather than to single still images, I think you would be placing a cost burden on systems which a lot of the smaller systems would not be able to withstand. Therefore, if you made anything like that mandatory, I think you would find there would be a lot of systems that could not comply because they simply could not afford to comply. That is not to say that in five or ten years' time that technology will not be cheap enough to be embodied, it might even be

11 December 1997] DR ROBERT BRAMLEY, MR RICHARD CHILDS,
MR SIMON HICKSON, MR PAUL PUGH, MS BRENDA HAWKYARD,
MR JIM ALDRIDGE, AND MR ROY THOMPSON

[Continued]

Lord Brain *contd.*]

within a shorter time, but at this moment in time authenticating, water-marking, encrypting, are still relatively expensive for CCTV images.

441. Thank you, but I think that raises two points. One is should, therefore, people who cannot afford a lot of money stay with, let us call it, tape-type imaging because that can be secured, and, secondly, if we do not start now designing the digital systems to meet the standards that you are suggesting could arise in ten years' time, we will be wasting a lot of money in the meantime because we will be putting in systems that will have to be replaced later? Am I right in making those two statements?

(*Mr Aldridge*) I think that most of the kind of technology which is being developed along these lines could well be added to existing systems. Today, the cost of modification might well be excessive, but I think that in terms of trying to promote the development of these, there is a great deal of development work already going on. In particular, within the broadcast industry there is huge pressure to develop new and much cheaper technologies. Where the problem lies is that most of the development of the technology is on what we would call the decoding end because if you are in the broadcasting mode, it is one-too-many and you want lots of people to be able to decode your images. It is the encoding end which is still expensive, but there are big developments taking place in that area and I think that in a relatively short period of time we will see some progress there.

442. So I think you are really talking now of the second part of the question, but should the Government do more to encourage these techniques at this early stage or should we encourage the Government to encourage the development of these techniques because I think, as was said earlier, there is a risk that the barristers will catch on to some of the doubts that modern technology gives rise to and one ought to be really prepared now or working hard to be able to allay those fears?

(*Mr Thompson*) If I may answer, my Lord, there are already systems which adopt digital recording technology. They are efficient systems and they have built into them exactly the kind of audit trails that we have already suggested are advisable. If these audit trails are insecure, then we feel that the eventual court process will throw out the evidence as being unreliable. We provide advice to the police and other security organisations in this country and we do feel that we are ahead of the problem. There is of course the private individual. The proliferation of digital cameras is tremendous, so—

443. Can I just pick you up on that word? Digital cameras, fine, but are they recording the information digitally or are they recording the digital information on tape?

(*Mr Thompson*) I am talking of digital still picture cameras.

444. I beg your pardon. Indeed.

(*Mr Thompson*) And of course we also have digital video cameras which record either directly on to a memory and then are downloaded at a later date on to disks or on to digital tape, so digital cameras are using tapes as well and some have the option of both.

I fear that we cannot control these devices being produced by the manufacturers in the Far East. I try to keep a file of all the new devices coming into this country and I am finding it very difficult because they are proliferating at a rapid rate.

Chairman

445. But taking that a step further, however this material is collected, do you see problems with presenting it in court?

(*Mr Thompson*) I do not see problems from the official point of view because we have already flagged the warning signs so that the systems which are already coming into operation now have audit trails built into them. There is a system at Heathrow, for example, which looks after the car parks and there will be electronic cameras on the M25 over a stretch for a trial period. You have had a submission from Dr Stephen Lewis who works with us on systems for encryption that seem to be secure using the kind of codes which are publicly available and these protect bank transactions. I do feel that there are going to be occasions when the court will receive an image which is taken by a member of the public who wishes to introduce this image into court in good faith and I believe it will soon be possible to bring in an expert witness who will look at this digital image. It has no audit trail, but it is presented by a member of the public of whom you have no reason to suggest that he has been mischievous in any way. An expert witness will look at it in terms of viewpoint, lighting, perspective and all these things and he will simply give a view as to the veracity of this image.

(*Dr Bramley*) I think we in the Forensic Science Service consider that that is an important role for the expert witness to assist the court in the evaluation of evidence, and it is a matter of assessing whether something is technologically possible, what skills are required, how long it would take to do things, what access to equipment would be required and what common sense applies. The court in the end makes the final decision as to whether something is acceptable and valid, but we are there to help them.

446. In your written evidence, you make reference to digital finger-printing systems where there will be no original copy and the courts will be expected to accept images from a digital source. Do you have any concerns at this stage? It is not in yet, as I understand it, but it is likely to come in.

(*Dr Bramley*) Yes.

447. So at this stage because there is an example of digital images being used in evidence without the benefit of the original copy, in the old-fashioned sense, once it has all been digitalised, what are your concerns there, if any, on the forensic side?

(*Dr Bramley*) I think there have to be some safeguards in the transmission of the image from the scene of the incident, if we are talking about collecting it at the scene of the incident, to where it is eventually captured in a controlled environment and you can start a proper audit trail.

448. Do you see that as an electronic audit trail or an administrative, documentary audit trail?

11 December 1997]

DR ROBERT BRAMLEY, MR RICHARD CHILDS,
MR SIMON HICKSON, MR PAUL PUGH, MS BRENDA HAWKYARD,
MR JIM ALDRIDGE, AND MR ROY THOMPSON

[Continued]

Chairman *contd.*]

(*Dr Bramley*) I think we will need both. For presentation in court, you need to be able to demonstrate how the image is captured, when it was captured, who captured it and you need to be able to show who has handled the exhibit. This is the normal continuity record which applies to all exhibits. You also need to be able to demonstrate how it was stored and how it was preserved to prevent corruption: was it exposed to magnetic fields, did anyone have the opportunity to get access to it. And you have got to be able to show through documentary records and electronic records what has been done to the exhibit, by whom and when. All of this is in common with all other evidence types. It is no different in these respects.

Lord Brain

449. Can I just go back to one small point? We were talking earlier about digital still cameras. With non-digital cameras, you have a film and you can see the frame before and the frame after and so on if you are given a "print". Do you think that the people, having received a digital print, ought to be advised to go back and look at, if they are available, the images on either side of the original print in the database and, if that is not available, at least be able to flag up that they have not been able to check this as part of their evidence?

(*Dr Bramley*) I think that we should always try to go back to as original an item as we possibly can. Sometimes there is no original item and you have to take peripheral evidence to show that something was authentic and that should be done as a matter of routine, yes.

Lord Flowers

450. A lot of emphasis has been placed by you and other people on the electronic audit trail. How easy is it to modify that? If you are an enthusiastic young man known as a hacker and you break into the Pentagon, you can presumably change the audit trail?

(*Mr Aldridge*) Well, I think that if you were really concerned about that, my Lord, one of the things you should be concerned about immediately is your bank account. In fact the use of a message authentication code (MAC), referred to in the Police Scientific Development Branch document that you have on traffic enforcement technology, uses exactly the same kind of coding used to protect banking transactions and, to the best of my knowledge, that has withstood and looks as if it is going to withstand any attacks. I think the advantages to someone attacking the system is a great deal more than perhaps—

Chairman

451. There was a Russian, was there not, Mr Leven(?), who managed to get into a bank in New York from Moscow. He was caught.

(*Mr Aldridge*) My Lord, I think someone was careless enough actually to give him their input password.

Lord Flowers

452. For the run-of-the-mill crime I am sure what you say is right, that the amount of effort you have to go through is simply too great, but for a real corker of a crime that might not be the case.

(*Mr Aldridge*) I think though that I still stand by what I said and I think the banks would stand by what they say, that the encryption techniques referred to in the PSDB document are solid. There is no indication at all that they can be broken or that they will be broken in the foreseeable future and I think that really if you genuinely felt that there was a major problem here, I think we should be bringing it to the attention of the banks straightaway because I think this has proved itself and it is a very effective protection.

Lord Howie of Troon

453. You say that the banks say the system is safe, but you would not expect them to say anything else, would you?

(*Mr Aldridge*) I think that if there was any indication that they thought it was not safe, we would be seeing moves for them to have it changed and there are no indications, as far as I am aware, that they are planning to change any of that, and this is not just used within the United Kingdom but is a worldwide type of process.

Lord Tombs

454. Can I turn now to city centre surveillance systems which are, I think, quite commonplace and have of course been encouraged by the Home Office. Do you have any figures for the total expenditure on such systems and have you done any assessments of their effects in reducing crime? Arising from that, is it still Home Office policy to encourage those systems as an effective and economic crime reduction policy?

(*Mr Childs*) Yes, I have some figures which might assist. There have been so far three challenge competitions from 1994 and another one has been announced for 1998/99. So far, excluding next year, £37.1 million has been spent on these schemes and there have been 553 winning schemes, and of those, 302 are currently operating. Next year, and the bidding guidance will be issued shortly, there will be £1 million worth of competition. The effectiveness of the schemes is a little bit difficult to be absolutely clear about because we are still fairly early into a lot of them because they take a long time to come on stream, but the implications that one can read into one or two local evaluations which have been done are that they do have an impact on crime and disorder, perhaps particularly disorder, but perhaps, in a sense saying there is jam tomorrow, the more recent schemes have required better evaluation tools within them. The indications are that those evaluation proposals are going to be quite useful at indicating success or otherwise. However, there are some caveats to put to this. The first is that it is very difficult to be absolutely certain that the CCTV cameras are the main reason for a change in offending behaviour because they are very often part of a complex picture of anti-crime measures that

11 December 1997]

DR ROBERT BRAMLEY, MR RICHARD CHILDS,
MR SIMON HICKSON, MR PAUL PUGH, MS BRENDA HAWKYARD,
MR JIM ALDRIDGE, AND MR ROY THOMPSON

[Continued]

Lord Tombs *contd.*]

have been put in place, so in summary of that, the indications are that they are successful, those that have been evaluated in local schemes, and I think in the future it will be possible to be more certain about that, looking at the way in which the evaluations is laid within them. The final point you raised was?

455. Is it continued policy?

(*Mr Childs*) It is certainly in the sense that a scheme has been announced for next year. I cannot comment on after next year, but certainly it is at the moment, yes.

456. Can I go back to the evaluation question and ask whether those are conducted by the necessarily enthusiastic people who put up the scheme or independent assessors and whether they usually take account of the possibility of displaced crimes?

(*Mr Childs*) They are done by a variety of people. Some are done by those involved, but others are not. I have personal experience of schemes where they are not done by those involved, but they are done by academics who have been brought in to do them. The displaced crime issue is considered in most that have done it, but again I have to say that the rigour that has been exercised on some of these evaluations might be open to question, but I think in the future things will be better, but these things do take time to show an impact on them.

457. One final question which interests me on that answer: is there a systematic variation between the independent assessments and the in-house assessments that you can discern?

(*Mr Childs*) I have not the vaguest idea, to be honest. I suspect I have a view, but I am not going to give it!

458. You can see my suspicion, can you not?

(*Mr Childs*) I do not know, is the answer. Ever was, though, ever was!

Chairman

459. Could we turn to the issue of modern technologies in data matching and the implications that this may have on privacy and public concern about a big brother approach. Is there a need for a policy in this area? Do you envisage the Home Office working up one? Has it worked up one?

(*Mr Hickson*) There is a policy on the processing use, exchange and disclosure of data which embraces data matching that is the comparison of different data collections. All those processes can pose risks to individuals' interests, either their sense of privacy or their actual welfare or finances. On the other hand, the processing of data is necessary for public and private organisations in the modern world. We already have a framework of law which attempts to balance those considerations, and imposes restraints on people who process or match data. As I mentioned earlier, its impact on CCTV systems is limited at the moment because of the way the law is defined, but it will increase through the imminent changes in the legislation.

Lord Nathan

460. In previous evidence from the Chief Constable, I was particularly interested to learn that he gave the example of the car entering the sliproad and being identified and that it might be convenient to identify that with an image of the same car which could easily be identified by the computer systems and the consequence of that was that it seemed to be taken for granted, and I do not question it, that the police would have access to material generated by the local authority dealing with the sliproad. What I wonder is how far does the law or do you consider that there could be movement of images with the same objective from the police and not just to the police? For instance, if you had a civil case of industrial espionage being conducted and it was important to secure the image of a vehicle or a person in a particular place, and that would be an important piece of evidence for one or other side in the civil proceedings, would it be appropriate for the police to be asked and to agree to hand over material which would enable that to happen?

(*Mr Hickson*) The philosophy underlying the present data protection information privacy law is essentially that where there is a good and legitimate reason, like the investigation of a particular crime, or the prevention of crime in particular cases, the exchange of data is reasonable and is proper. What the law tries to stop is simple fishing expeditions data matching for no obvious legitimate reason. There is a lot more detail to it, but that is the basic principle.

461. The tendency of what you are saying is that it would be perfectly proper for material to be supplied to the police in a prosecution which they were getting under way, but perhaps it would not be appropriate for the police to give material to a private concern with a view to pursuing a civil remedy in the courts as opposed to a criminal one, though it might be equally relevant from the point of view of the contestants in the case.

(*Mr Pugh*) Yes, and perhaps I might add to that from an operational policing point of view. I think similar considerations arise in relation to the general issue of disclosure of information held by the police to other parties. To give another example which I think is in some senses analogous, the question has arisen recently in the context of information held by the police in relation to sex offenders in the community, for example, and whether it is proper for information held by the police to be made available to third parties. Now, the general position in this, and it is not, as it were, codified in statute, but there is a generally understood common law duty of confidentiality on the police in relation to the information which they obtain in the context of the enforcement of the law. They would not generally, they would not as a matter of routine disclose to other persons and they, like everybody else in a sense, are bound by the provisions of the European Convention on Human Rights in relation to privacy in that respect. However, that is with the proviso that where they take a considered and appropriate judgment that the disclosure of a particular piece of information is necessary for the purposes of the prevention or detection of crime, then they are able to do that. Now, the question of whether or not the

11 December 1997]

DR ROBERT BRAMLEY, MR RICHARD CHILDS,
MR SIMON HICKSON, MR PAUL PUGH, MS BRENDA HAWKYARD,
MR JIM ALDRIDGE, AND MR ROY THOMPSON

[Continued]

Lord Nathan *contd.*]

disclosure of a particular piece of information is appropriate for the prevention and detection of crime is a judgment which can only be taken on a case-by-case basis and that was a principle which the courts have recently supported in the context of information released about some convicted sex offenders.

(*Mr Childs*) I think the issue you raised in your question was about a civil action. If one excludes completely from consideration of the issue the criminal aspect and you go to, for example, precedents that are set by road traffic accidents and copies of police reports on road traffic accidents, which are entirely civil matters if one excludes the driver, those are made available to insurance companies and they are made available to other people. Where police officers get called to disputes in private property, if there is a subpoena from a county court or a civil court for the production of police reports, providing they are not covered by privilege which they would not generally be, then police officers can be called to give evidence and produce what evidence they have which is available. I am a little rusty on the detail of it, I have to say, but, as a broad principle, the police will make evidence available if it is not covered by privilege for civil proceedings. I think that is right, Paul, is it not?

(*Mr Pugh*) Yes, subject again to a judgment as to whether it is appropriate in a particular case. It is difficult to make generalisations because they in a sense have to make an assessment as to whether the disclosure of information is justified in these particular circumstances.

Chairman

462. On that business of disclosure of information, I am thinking now of a different area and that is where the police release information to the media perhaps for road safety reasons as opposed to looking to try and find a potential criminal. Is there a policy at government policy level about that or is it entirely left to the individual police forces and the local authorities? Is there a feeling that there should be because clearly more and more material of this sort is going to become available? I just wondered whether in the Home Office this had been given any thought or whether you had any views about it which could help our own thinking.

(*Mr Pugh*) I am not quite sure about the context which we are talking about here, but certainly—

463. Well, the context here is really that closed circuit television and other systems like that have a value to law enforcement and ultimately may be used in courts. That value could be undermined if there was a public perception that these systems were going to be used in other criminal law enforcement ways.

(*Mr Pugh*) Do you mean things like TV programmes where they are using police material?

464. Yes, that is a for instance and I just wondered whether there was a feeling that because the public confidence in these systems, if that public confidence remains, is going to be important to their value in law enforcement and indeed the deterrence of crime, the public acceptability is a very important thing and we want to be very careful that nothing undermines

public confidence in CCTV-type systems. One feeling might be that the material is being used in a way which is an invasion of privacy or is seen to be unacceptable or viewed by some to be unacceptable. At the moment what I am really looking for is whether there has been any Home Office thought given to this and whether it is perceived as a potential problem or that it is a problem. I am just looking for a view from Mr Childs or any of his colleagues on that.

(*Mr Pugh*) Well, the very broad issue I do not think we have looked at as you define it in that sense, but we have done and are doing work on some relevant issues. I think perhaps one of the difficulties in answering the question is that we are approaching it from different angles. For example, as we touched on a minute ago, the general question of disclosure of information between agencies, including the police, for the purposes of protecting the public, that is an issue about which ministers are concerned and which they have asked us to look at: about whether there is relevant information, whether collected by CCTV or indeed criminal investigation, for other purposes which different agencies hold about potential or indeed convicted offenders which might be usefully shared with other agencies for the purposes of protecting the public, so that is one aspect which ministers are concerned about. Another aspect which they have asked us to give some consideration to with the Association of Chief Police Officers is the issue of the contact between the police and the media in the context of particular criminal proceedings, whether information should or should not be made available to the media and, for example, the question of the media being present at raids is one that has given rise to some concern and that question of police-media interface is one that ministers have asked us to look at, as I say, with chief officers. As to the very broad issue that you raise, particularly in the context of CCTV, whether there is a clear policy on what should or should not be done with CCTV pictures, expressed in those terms, it is certainly not one on which I am aware of there being a clear or coherent policy development.

(*Mr Childs*) I think that I might be able to find out very rapidly if the guidelines actually cover that issue. From my recollection of them, they do cover the distribution of information that is obtained from the kind of CCTV system we have been discussing, that is, available in public places, but that it will not be made available to third parties for the reasons you have identified, the confidence that this stuff is not just floated around and generally made available.

Baroness Hogg

465. If that is the case, the fact that it is presently being shown on television suggests it is not at all in breach of the guidelines.

(*Mr Childs*) Yes.

(*Mr Hickson*) Those programmes I have seen have the number-plates blanked out, so there is no obvious route to identify the people concerned. If it is simply for educational purposes, then typically scenes are taken to observe individual confidentiality.

11 December 1997]

DR ROBERT BRAMLEY, MR RICHARD CHILDS,
MR SIMON HICKSON, MR PAUL PUGH, MS BRENDA HAWKYARD,
MR JIM ALDRIDGE, AND MR ROY THOMPSON

[Continued

Baroness Hogg *contd.*]

That is quite different from the investigation of particular offences.

(*Mr Childs*) If I could just cover the point about making stuff available at the moment, the ACPO policy on that is clear, that it is not encouraged, and the advice that ACPO has put is that it does not do it. That goes to the interesting issue of what is an operational and independent act by a chief constable and what is not of course which may be the reason for some of the excerpts getting out. It also may be that some of them got out a very long time ago and actually they are not being released now and that, I think, is also an issue. Of course a lot of it does not come from this country in fact, it comes from abroad, certainly some of the clips I have seen of late.

Lord Brain

466. We, I think, have all watched *Crimewatch*. There images very often are released to help the police solve a crime, quite justifiably. Is there any feeling that care needs to be taken so that it might not prejudice some future important jury trial or something like that? Is this something where the police watch themselves very carefully or are there guidelines on it?

(*Mr Childs*) My experience is that it would not be issued without the agreement of the Crown Prosecution Service in those circumstances, or at least their advice would have to be obtained. I do not know if one of my colleagues can add to that.

(*Mr Pugh*) Again I think the same principle applies as to any piece of conceivably relevant evidence that the police may hold. I think that they would as a matter of course have full and proper regard to whether the question of releasing information which they may hold relevant to a crime in advance of having, as it were, apprehended the convicted person what impact that might or might not have on any subsequent proceedings and I think in a sense that seems to be such a self-evident principle, I do not think it is one on which there is sort of written guidance because it seems so axiomatic.

(*Mr Childs*) It would be very difficult to have one rule for it because there might be so extreme a crime that the only evidence you had you needed to advertise and any prohibition of that might actually—

467. I was not saying a prohibition, but I was just trying to see if there was a uniformity or whether it is up to each police force on things like that.

(*Mr Childs*) I think there are 43 variations of uniformity!

(*Ms Hawkyard*) The guidelines, to which reference has been made, were issued in 1984 and will be superseded when the provisions of the Police Act 1997 come into force. They contain guidance on the retention and use of product of surveillance, including the use of video cameras. This states that such recordings should only be retained for as long as

required by the circumstances of the enquiry, or by any subsequent court proceedings, and may only be used for such purposes with the authority of the person who authorised the surveillance in the first place.

Baroness Hogg

468. But there is no reference to the permission of the person who is covered in the material?

(*Ms Hawkyard*) No, it is only the person who authorised the use of the equipment in the first place.

Chairman

469. I wonder if this, Dr Bramley, is more for you and the Forensic Science Service, and that is your perception of the court's understanding of these modern technologies. I know that not only the court, but all those who handle evidence get advice from you on a variety of issues. I wondered whether that is happening now in the digital imaging area or whether in fact it has been happening for some time or whether you see it as a growing need.

(*Dr Bramley*) I think that is a growing need. You may be aware that we work very closely with the Crown Prosecution Service and the police to give them training and to make them aware of technological advances, notably in recent times with DNA, and we are producing a lot of information for the courts, lawyers, the police and the Crown Prosecution Service itself to enable them to understand what the advances in technology are, what the limitations are, how it should be used, because the presentation of this evidence in court is vitally important if it is not to be thrown out. I feel there is a need, probably for the Forensic Science Service, it is our position, to provide some sort of educational material and training to the appropriate people who need to know about it.

Lord Tombs

470. Would that include defence lawyers?

(*Dr Bramley*) It would indeed. The Forensic Science Service in fact offers its services for the prosecution and the defence. We are totally impartial.

Lord Tombs] Very good.

Chairman

471. Any further questions? Anyway the time, I fear, has run out. Are there any concluding remarks which you, Mr Childs, or any of your colleagues would like to make before we end this session?

(*Mr Childs*) I think not, no.

Chairman] Thank you very much indeed to one and all of you for coming to see us. We are very grateful.

WRITTEN EVIDENCE

Memorandum by Security Facilities Executive (SAFE)

Security Facilities Executive is an Agency of the Cabinet Office (Office of Public Service), our role is to provide physical security advice to Government and the wider Public Sector. Our expertise in the area of digital images is based on our experience with CCTV on the Government estate and with Local Authorities on town centre schemes.

We have considerable knowledge of state of the art and commercially available CCTV equipment as applicable to our main areas of advice which cover counter terrorism, counter espionage and general crime.

The following refers to questions posed by the Sub-Committee:

1. What is the current and forecast use of digital technology for image collection, storage and transmission? What is its use by the courts and legal profession? What is the state of the art of image manipulation.

1.1 Current charge coupled device (CCD) cameras already use digital technology for image collection which is then generally converted to an analogue signal for transmission and recording. There is already a move to replace analogue recording with digital methods with storage on hard disc or tape and eventually to optical discs. The use of digital technology for image collection, storage and transmission will certainly increase in the future.

1.2 Both prosecution and defence already use digital enhancement for recordings used as evidence.

1.3 There are many off-the-shelf packages already available for image manipulation. Enhancement involving contrast, noise removal or colour information operations are more successful than electronic zoom operations (to increase the size of part of the image). Because of the set up of the camera and CCTV system (especially fixed systems) electronic zoom operations are usually the operation that law enforcement officers ask for.

2. Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean they should be treated differently when used as evidence?

2.1 Yes. Copied, manipulated (tampered) enhanced images should be stated as such in evidence (statement) at court and *any* alteration or enhancement should be supported by an audit trail produced at the time.

Ideally an encrypted audit trail similar to that provided by IMPROVE (an enhancement software package produced by the Home Office Police Scientific Development Branch) should be used.

Any recording medium (tapes, diskettes etc) should be subject to the usual continuity procedures for court evidence (sealed tamper evident packaging, log book audit trail and signatures of all persons handling the items with dates and times).

3. Would special measures to authenticate digital images, eg watermarking, increase their utility as Evidence? What would be the preferred practical measure?

3.1 Watermarking may only be useful in identifying the source. If the evidence has been handled with full continuity procedures then there may not be a problem.

3.2 Current technologies would need to be evaluated if this aspect is to be taken forward. SAFE has no further information available at this time.

4. Under what circumstances and with what controls should modified or enhanced images be used as evidence?

4.1 Modified or enhanced images should be used where the original image is of poor quality and it can be improved by enhancement (eg noise removal, contrast adjustments). Ideally the image from the camera/CCTV system should be such that enhancement is not required. Enhancement should only be used as a last resort and should be subject to continuity and audit trail statements.

5. Do technologies which compress data or use error correction technology when transmitting it raise special problems?

5.1 Compression and any other manipulation of the image increases the possibility of introducing errors. We believe there may already be some recommendations in place suggesting that compressed and expanded images should not be used as evidence.

6. Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?

6.1 Image tracking should not threaten civil liberties any more than current CCTV systems provided that their deployment is advertised, the operators are trained and appropriate controls of the recorded image are in place.

7. Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?

7.1 The principle of CCTV surveillance systems is for public safety and security and not to spy or infringe civil liberties. The placement and use of cameras should possibly be controlled to some extent but we should maintain the option of placement and use in any area where the perceived threat is appropriately high. The release of information obtained from CCTV systems should definitely be controlled, some recent media presentations of recordings has caused public concern.

8. Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?

8.1 Yes. Courts and law enforcement officers should be aware of and updated on the technology of digital imaging and manipulation. It may be that those who are aware of the limitations of enhancement will tend to interpret the video information themselves and attempt to become the "video expert" and rightly or wrongly make judgements regarding video evidence.

9. Is there the need for special measures to control the publication of modified images by the media?

9.1 We believe that there should be strict controls on the publication of any images from any CCTV surveillance system covering areas accessible to the public. Uncontrolled publication is likely to reduce public acceptance of surveillance systems generally.

Dr N D E Custance
Consultancy Director

Memorandum by Mr Grady Miller, Trade Policy Analyst

INTRODUCTION

This memorandum is being written pursuant to a request from the Select Committee on Science and Technology concerning several issues on whether or not computer generated digital images and under what circumstances should be used as evidence in, one assumes, United Kingdom courts of law. The committee requests submissions on several aspects of the use of digital imagery and matters arising from both internal and external control of image data generation covering matters of surveillance and civil liberties and the consequent collection of image data as proof of facts.

It is not intended in this paper to address all of those issues for which the committee is concerned but to concentrate on items 1–6 where the key thread of inquiry involves the ability of the proponents of digital images to persuade audiences of the veracity of images selected.

In this particular instance the inquiry is a bit tardy. Digital imagery in the form of animations, simulations and reconstructions has certainly since the late 1980's been admissible as types of evidence in American courts such as charts, maps and diagrams have been historically used. Furthermore, were the state of English law of evidence completely undeveloped in this regard, evidence by way of comparative law would have begun to fill the gaps in practice. Therefore the question of whether or not digital imagery ought to be admissible as evidence has been answered. The real problems of visual imagery as tools of persuasion in the hands of the general public whose purpose in collecting and using image data is as diverse as the populations in which computers are found and only slightly different from cartographers who recognise that a map without a viewpoint would not sell.

MANIPULATION

1. Visual image perceptions as psychophysical phenomena are not well understood though well studied. As for triers of facts in the common law tradition it is well settled that juries tend to believe what they see. What they see in an evidentiary presentation will vary according to their own personal experiences, their belief systems, social and peer pressure and their interest in the subject matter. It then becomes obvious that some will make assumptions about the state of reality depicted and these assumptions, being out of court evidence should be, if discovered or detected, excluded as bias if not hearsay evidence. This behavior for both fortunate and unfortunate reasons is the very characteristic that juries are chosen for, their ordinary experience of life. This behavior will occur even if the most objective standards of presentation are aimed for.

2. Recent research has demonstrated that visual perception has cognitively natural levels of discrimination and organisation. This research has shown that over time and in a large sample perceivers of visuals can and do find order, symmetry, patterns and make sense of visual images without the assistance of the presenter. Research has also shown that his ability is probably limited to simple diagrams and depictions. A digital image presentation in court would most likely use complex colour, perspective and magnification of facts and relationships outside of the experience of most jurors but the state of this art is available to any artist, photographer or writer or scientist. Therefore confusion and misapprehension on the part of the audience seems to be inherent in visual presentations. This occurs whether or not the image is digitised but digitised images are not a representation but a "telepresentation" which itself is a distortion of reality. Without manipulation no presentation could be made or perhaps be worth presenting.

3. A more important issue is for what purposes are the propounders of the visual images advocating their use: as proof of facts (substantive) or as assistance to argument (demonstrative). On this issue the American courts are of little assistance and their experience has shown both conflicts and little policy consistency sometimes siding with the theorists where the scientific method is established or the newer angle where the presentation would aid in the resolution of issues in contention. The problem is demonstrated by recent investigations into the Lockean problem of whether "texture" is a primary or secondary element of matter. The hypothesis being if texture is primary this elemental character would be demonstrated by x-ray crystallography. This aspect of matter is not ordinarily a problem for laymen as visual inspection of material would normally elicit agreement among laypersons. Under investigation it appears that both colour and texture are secondary aspects of matter and that a presentation which offered to prove a piece of evidence is of one substance only by its visual texture should fail to establish that fact. There is no question that a jury would be more impressed and receptive to a presentation which compared tree bark with alligator skin. This itself is not an issue of manipulation but the one of obtaining meaning from images generally.

AUDIT TRAILS

4. Any evidence compiled outside of the courtroom is cast in the light of hearsay and is presumptively suspect unless it meets with a fairly well established exception. Copies of evidence are also suspected as not the best evidence available unless also corroborated by the person who actually made the record and originals cannot be produced. Computer programs and such have been admitted by American courts as exemplars of business records and thus an exception to hearsay exclusions. In these cases problems of authentication are minimal because any autonomous program operation can be verified by an outsider and the data so compiled rechecked. Visual images are different as they reflect a point of view and an audit trail for images unlike for Email records of access produces only a record of possible re-projection as sight perception is a secondary aspect of reality.

5. Secondary evidence then is perhaps suitable as argument and an audit trail merely compiles a record of custody but provides no further dimension of soundness because technology is, at this point incapable of verifying the underlying image as real. The use of color spectroscopy in element identification is perhaps illustrative of some of the problems in that while dictionary standards of color composition are now accepted, color spectroscopy like texture does not reveal itself in crystallography. An audit trail would have to relate to foundational relevancy within a hearsay exception. It is thus proposed that the dangers of copying, tapering and manipulation of digital images is not a true danger in that the image projection can not be substantive proof of anything.

AUTHENTICATION

6. Authenticity of evidence raises concerns about its origins and authorship and the committee queries whether marks and signs would assist in verifying origin. This is a difficult aspect and has many sides not the least of which relate to disputes even among trade mark holders of established marks and some recent controversy over the authenticity of fingerprinting techniques. To their credit courts have long resorted to expert validation of evidence offered as proof. In American courts the most besieged experts are the scientific ones whose expertise is now open to challenge by changes in the Federal Rules of Evidence where experimental technology runs ahead of the scientific method to prove science fiction as facts, reflecting a new precedent set by the Daubert case.

7. Two problems of authentication come to mind. The most famous case involving digital manipulation was effected by the National Geographical magazine cover of the pyramids in Egypt. The monuments were shown to be close together in the same photo. Clearly expert testimony would be needed to impeach such a display not because of the falsity of the images themselves but because of the depicted spatial relationship shown by the photo. This expertise would be most likely geographical but not archeological and another expert could indeed verify the existence of the monuments situated in Egypt. What science cannot do but experimental digital visualization can is to show that they might have been at one point in time closer together or hewn from the same source or were part of a common design. Thus authentication seems to be a relative aspect of evidence with limited probative value. It could be said that authentication is thrown out as tool where the assumptions and techniques of the scientific method reveal less than other techniques.

8. The other part of the problem is cross examination. Authentication is not a one dimensional process. Digital visualizations have interpenetrated all scientific and technological areas and raises as many questions as it answers, teaching something new to all who use them. They are said to create new facts as they go along. These new facts unlike the static assumptions of the scientifically produced methods become independent witnesses not accountable to counsel or to any community. The legal and research community, aware of the ability of technology to create new models, try to address the issue of authentication within an identifiable scientific group which may claim it. As these are often on the cutting edge of research and rivals to established groups, widespread acceptance of their conclusions is not a given and the probative value of such testimony remains a trial strategy.

MODIFIED OR ENHANCED IMAGES

9. Digital images represent a quite enhanced version of photographic impression and of X-ray imagery. Both forms can be rendered into digital format. What is not widely known is that x-rays have a moving format much like motion pictures and moving x-rays are often used in surgery and in this format only black and white images were thought to be necessary for surgeons. On the other hand, the addition of deeper color added to photographs of OJ Simpson's photo images were achieved digitally, with the expectation that a more sinister impression in an out of court context could be created. One tends to think of older technology as a more truthful and reliable form of evidence. Photographic impressions required light sensitive chemicals in order to produce an image. Digital visualisations require direct manipulation of an energy field without prior form. The issue of modification or enhancement by the addition of color does not answer the underlying question of whether the image projected is the truth. We have already shown that color, texture and indeed all visual sense impressions relay secondary rather than primary information.

10. Therefore the issue of whether or not controls are necessary for introduction of digital evidence turns on whether the proponent seeks their admission as proof of facts or as argument. Modified and enhanced images clearly relay information which is not necessarily intuitively obvious nor necessarily prejudicial or inflammatory. Moving X-rays pictures which exclude the sense impression of colour are an esthetic deprivation of sensation with no more ability to reveal truth as is its addition to create an aura of villainy. The cultural milieu of the viewers of digital images is at least as important as the image. For older surgeons the precision of the attempted procedure dealt with their skill level in performing an operation. Provided that the relevant areas were sufficiently luminescent, the procedure could be carried out in reasonable confidence. However, when facts are at a premium or still to be determined then the motivation to resort to sensate "facts" is strong because primary facts may not be capable of establishment and secondary facts become the best evidence available.

11. The element of esthetics rather than information generation is probably more of a force in driving digitalization due possibly to the capacity for interaction for the viewer. Interaction rather than scientific exploration is perhaps a better teacher because it produces experience directly. Therefore a restriction on the triers of facts that they leave matters of image complexity to experts or that their presentation must only contain modest and unrefined imagery must imply that truth is naked and bare. Courts in the US have been sympathetic to this appeal in the sense that understanding the argument propounded aids in resolutions of controversies provided the visual image is propounded as argument. This should be perhaps its only control subject to the contingency of robust rebuttal.

SURVEILLANCE AND CIVIL LIBERTIES

12. The arguments concerning compiling of digital images under conditions of surveillance which possibly violate civil liberties are especially vexed when there is no established right of privacy. One can distinguish between invitees, those who venture into public and/or private property but who are presumed to be on the business which is of interest to the landholder and those persons who are merely on the public roads and right of ways. The latter perhaps have more grounds for grievance because they are on no other business except their own. Surveillance of these individuals is an affront to their freedom as only captives can be viewed indiscriminately and at the will of another. Therefore systematic viewing of individuals without their knowledge is incompatible with freedom. The problem is not settled because on one hand private interests do it or on the other hand, civil authorities carry it out.

13. In either case whether or not the compilation results in a disclosure to third parties for public or private interests the collection has sinister implications. A) the compilation takes place without the subjects participation; B) the subject cannot object to or cross examine the images once compiled; C) the purpose of the compilation is to deprive the subject of complete freedom of movement; D) the images themselves may or may not be proof of any fact alleged therein; E) A regulation which allowed for widespread and systematic collation of visual data on people is the foundation regulation for the exercise of tyranny. This may be justified for public or private landholders but public roads and streets bring special social pressure to bear on individuals or groups and images of the prisoner's dilemma come to mind.

14. The prisoner's dilemma is a game strategy where at least two parties are being accused of criminal joint behaviour. The authorities pressure both to confess while informing one that the other has given additional evidence against him. Unknown to him, what evidence the authorities hold is insubstantial but as he is urged to save himself alone, he provides in a confession the only admissible evidence there is in the case.

15. The case against this type evidential gathering again refers to whether or not the data is to be admitted as substantive or as argument. Either way the coercive capacity of the systematic non challengeable compiling of data on the movements of free people is not lessened by their putative right to demand its access such as with credit reporting agencies. Comparative American law would show that credit reporting agencies, under a duty not to report or to collect unsubstantiated data have frequent defamation suits brought by consumers under state and federal Fair Debt and Collection Acts about evidence known to be false to the collectors. This is true even of large money centre banks whose consumer operations are small by comparison to their international dealings. For these banks such suits are a cost of doing business.

16. Comparative American law further shows at least one theory under which systematic compilation of records seeks to be admitted. That is the “silent witness” doctrine. Under this doctrine, the propounder of recording device evidence must demonstrate the accuracy of the device. This is one of the variations of business record hearsay exception where authentication is made by the persons who are normally present when the information is transmitted. The general trend of American rules for computer generated evidence tends not to have elevated digital data to a heights of “scientific” demonstration but allow existing rules of procedure to interplay with advanced technology.

CONCLUSION AND TRADE POLICY IMPLICATIONS

17. The state of the art of image manipulation has brought science fiction and fairy tale depiction into many aspects of modern life with the attendant dangers of being able to purchase virtual reality kits for interactive experience and court room testimony. In some cases digital imagery has ousted science as a basis for proof of facts and in others has supported a revised ontological explanation of the human experience. The law has simply not kept pace with these developments in many instances because some of it is not well understood.

18. The most important trade policy implication for this technological innovation appears to increase the possibilities for commercial espionage, some prospects of crime deterrence and detection but more pressingly is the deterrence of free movement of workers in the European Community. Widespread citizen surveillance would have been an experience of Eastern Germans where neighbours and family acted as silent and often reliable witnesses for the state.

July 1997

REFERENCES

- D Saracend, “Creating Demonstrative Evidence”, 14 California Lawyer 59(3) Dec 94.
- N Chatterjee, “Admitting Computer Animations”, 62 Defense Counsel Journal 36-44; Jan 95.
- S Kurzban, “Authentication of Computer Generated Evidence in US Federal Courts”, 35 Idea 437-460.
- M Borelli, “The Computer Advocate”, 71 Indiana Law Journal 439-456 Spring 96.
- F Marchese, *Understanding Images: Finding Meaning in Digital Imagery*, Santa Clara: Springer Verlag, 1995.

Letter and Memorandum from the Press Complaints Commission

You will have seen that the issue of electronic enhancement of pictures by newspapers (covered by your question 9) is an issue that has come very much to the fore in the last few days. As a result of this, the Press Complaints Commission will be reviewing the whole issue in due course to see whether it has any recommendations to make to the Editors’ Code Committee about changes to the industry’s Code of Practice.

I thought it would therefore be useful to set out these points in a formal answer to question 9—which, as you rightly say, is the only one directly relevant to the PCC. This is attached.

QUESTION 9

Electronic modification of images by newspapers and magazines

At present, the issue of electronic modification of images is dealt with under Clause 1 (Accuracy) of the industry’s Code of Practice. Under the terms of the Clause, individuals whose images have been altered can bring a complaint that an image is “misleading or distorted.”

There has been no evidence to date that this is a significant problem—although the Commission did receive a complaint about a picture which raised this issue last year. After investigation, it decided that there had been a breach of the Code because of the misleading nature of the pictures. A copy of that adjudication is also attached for the Committee’s reference.

However, in the light of recent events—and concern over electronic manipulation of pictures of Diana, Princess of Wales—the Commission will now look at the issue in more detail to see if it needs to issue fresh guidelines to editors on the matter, or to see whether it needs to recommend to the Editors’ Code Committee any changes to the industry’s Code of Practice.

The Commission will keep the Committee in touch with any developments on the issue.

15 August 1997

Memorandum submitted by Symonds Group Ltd

Q1. What is the current and forecast future use of digital technology for image collection, storage and transmission? What is its use by the courts and the legal profession? What is the state of the art of image manipulation?

A1. We are in an age where digital technology has evolved from being a primitive tool principally with an entertainment value to an essential aid to daily professional activities. The reliance on such technologies to simplify our tasks is becoming increasingly total.

The current market requirements are for digital interconnectivity, high speed communication links and interactively. Demands exist within this market for computer networks and systems not to be constrained by boundaries or formats but to integrate and communicate. Under the "Digital Super Highway" banner the communications market is forging the way forward for a secure high speed digital infrastructure. Examples of note are the ease with which the internet can now be accessed and the recent ability to conduct "safe" money transactions.

The trend is for open system architecture and total system integration within organisations to improve overall company efficiency by ensuring easy access and fingertip control. This trend coupled with consumer demands for instant and simplified access to stored data are not satisfied by the capabilities of analogue systems.

Digital transmission is currently available and is used in many business applications. Digital storage is currently available and usable. Capacity of media is increasing along with reducing costs. The feasibility and practicality of digital storage usage is proportional to the compression method deployed.

We recognise that the courts and the legal profession will be increasingly presented with digital evidence, this we see as inevitable as a replacement to video evidence.

Image manipulation has been available to professionals since the early days of photography. It evolved with the advent of moving pictures and then again with the introduction of video. It is therefore not a new problem.

With recent increase in computing power at affordable prices and improvements in imaging hardware, image manipulation has become far more accessible.

Q2. Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean they should be treated differently when used as evidence?

A2. As with the requirements for speed detection devices to have a Type Approval by the Home Secretary for evidence to be admissible in support of a prosecution for exceeding the mandated speed limit, a similar requirement should, we feel, be imposed on digital recording. With similar procedures in place the robustness of digital image evidence may be considered in the same way in presentation as any other form of evidence.

Q3. Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence? What would be the preferred practical measure?

A3. There are many techniques available to "authenticate" digital images and many tamper proof storage media currently available in the market, ie "Write Once Read Many" to strengthen the authenticity of digital images and data. The validity and requirements for such techniques we feel can only be satisfactorily addressed with the introduction of a Type Approval or similar process.

Q4. Under what circumstances and with what controls should modified or enhanced images be used as evidence?

A4. We have indicated previously that we feel the presentation of digital evidence should be in accordance with a clearly defined framework, typically consistent with Home Office Type Approval. Given the establishment of a suitable framework, controls in respect of modified or enhanced images will be inherent within the procedures, ie evidence when presented can be certified as being compliant with the relevant process.

Q5. Do technologies which compress data or use error correction technology when transmitting it raise special problems?

A5. Data compression is a complex area of mathematical equations. Every technique has its requirements for checks and error correction technologies. Acceptable methods and technologies can best be handled under a Type Approval process.

Q6. Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?

A6. Widespread introduction of surveillance cameras does in our view have major implications on civil liberties. If cameras are used in conjunction with image tracking software then the effectiveness of surveillance is vastly improved and thus the implications on civil liberties increased.

The way in which surveillance cameras and associated software are used and the controls placed on the consequential information is we believe fundamental to the impact these emerging techniques will have on civil liberties.

If surveillance facilities are managed and operated within an appropriate framework scope exists for any threat to civil liberties to be transferred to a benefit. The enhancement in security made possible by the appropriate use of surveillance techniques can improve personal safety and in this way improve an individual's right to move freely and safely in public spaces.

Q7. Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?

A7. For surveillance cameras to continue to receive public support and to deliver the potential benefits, we believe strict statutory controls should be introduced to govern their placement, use, and access to consequential information. Scope may exist for incorporating these requirements within the framework of existing legislation; typically the Data Protection Act.

We believe that operators and managers of surveillance systems be registered/licensed. Conditions of the registration/license should only allow dissemination of images within the scope and purpose for which the license/registration is granted. It would greatly assist the industry if designers of public area CCTV facilities were required to formerly register and receive approval for, the intent of surveillance systems prior to their detailed design, tender and installation.

Q8. Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?

A8. We have indicated that we believe the appropriate way forward is to parallel existing Home Office Type Approval procedures for the gathering, storage and distribution of digital evidence. If this approach is adopted, then it is essential that law enforcement officers and courts are made aware of the procedures.

In respect of training on the technical limitations of digital technology and acceptable evidence from digital images is we feel a too complex and rapidly developing subject to realistically keep all law enforcement officers and courts updated on developments. It is therefore more practical for say a department within the Crown Prosecution Service to authenticate digital evidence before it is presented to the Courts.

This authentication/approval process will we suggest, confirm that the equipment used to gather the evidence is itself approved and all necessary documentation exists.

Q9. Is there the need for special measures to control the publication of modified images by the media?

A9. We believe that special measures to control the publication of modified images by the media should be put in place. Restricting use of data via a license mechanism will place effective restrictions on the dissemination of information. If an audit trail is mandated back to the original then the status of images can be determined.

David J Robertson
Omer Kadir

8 September 1997

Memorandum by Broadcasting Standards Commission

According to the Broadcasting Act 1996 the Broadcasting Standards Commission is required to draw up a code giving guidance as to the principles to be observed and practices to be followed in connection with the avoidance of:

- (a) unjust or unfair treatment in programmes; or
- (b) unwarranted infringement of privacy in, or in connection with the obtaining of material included in, such programmes.

This Code (in its current draft form) is submitted as evidence to the Sub-Committee.

In addition the Commission has drawn up a code on standards of taste and decency in television and radio.

It is from these codes, and the material which supports the guidance given within them, that the particular evidence given here is drawn, particularly with relation to Questions 6 and 9.

Q6: Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?

The issue of public interest is deemed to be key, especially if material is obtained either through deception or misrepresentation. The use of CCTV would be a threat to personal freedoms if this issue were not seen to be fundamental to the justification for using those images.

The draft code on fairness and privacy states:

“Factual programme makers should not normally obtain or seek information or pictures through misrepresentation or deception, except where the disclosure is believed to serve an overriding public interest and the material cannot reasonably be obtained by any other means. Where the use of deception is judged permissible, it should always be proportionate to the alleged wrongdoing and should wherever possible avoid the encouragement of conduct which might not have occurred at all but for the intervention of the programme-maker. Prior editorial approval at the most senior editorial levels within the broadcasting organisation should be obtained for such methods. The programme should also normally make clear to the audience the means used to obtain access to the information, unless this places sources at risk.”

The use of images from surveillance cameras which capture moments of public importance in private people's lives should be used sparingly and as appropriate to the point in time they capture. The draft code on fairness and privacy states:

“For most of the time, the private lives of most people are of no legitimate public interest. It is important that when, for a short time, people are caught up, however involuntary, in events which have a place in the news, their situation is not abused or exploited either at the time or in later programmes which revisit those events.”

In addition public research conducted among survivors of tragedies for the Commission¹ illustrates the great distress the repeated use of these images can cause. While it was accepted that there would be renewed public interest at the time of a trial or an inquest, it was a difficult time for survivors. As one person said: “Once it got to the trial six months later, I had it all being brought up again . . . and the same photos being shown. It was like reliving the whole thing again. They could have kept a lower profile for the family's sake. At that second stage, six months later . . . when we were trying to get ourselves together we could have done without the whole thing again.”

With reference to the use of hidden microphones and cameras, the draft code is quite specific:

“The use of secret recording should only be considered where it is necessary to the credibility and authenticity of the story, as the use of hidden recording techniques can both be unfair to those recorded as well as infringe their privacy. In seeking to determine whether an infringement of privacy is warranted, the Commission will consider the following guiding principles:

- (i) Normally, broadcasters on location should operate only in public where they can be seen. Where recording does take place secretly in public places, the intended use of the words or images recorded should be sufficiently in the public interest or the public domain to justify:
 - the decision to gather the material;
 - the actual recording; and
 - the broadcast
- (ii) An unattended recording device should not be left on private property without the full and informed consent of the occupiers or their agent unless seeking permission might frustrate the investigation by the programme-maker of matters of an overriding public interest.
- (iii) The open and apparent use of cameras or recording devices on public property when the subject is on private property must be appropriate to the importance or nature of the story. The broadcaster should intrude unnecessarily on private behaviour.

When broadcasting material obtained secretly, whether in public or on private property, broadcasters should take care not to infringe the privacy of bystanders who may be caught inadvertently in the recording. Wherever possible, the identity of innocent parties should be obscured.

Broadcasters should apply the same rules to material shot secretly by others as they do to their own recordings in taking the decision whether to broadcast the material.

When secret recording is undertaken as part of an entertainment programme, care should also be taken to prevent the unwarranted infringement of privacy. The people who are the subjects of a recorded deception

¹ Survivors and the Media, Ann Shearer; BSC Monograph No. 2, 1991.

should be asked to give their consent before the material is broadcast. If they become aware of the recording and ask for it to stop, their wishes should be respected. In a live broadcast, especial care should be taken to avoid offence to the individuals concerned."

Q9: Is there a need for special measures to control the publication of modified images by the media?

The draft code on fairness and privacy described above illustrates the perceived need for special measures to be adopted for the use of images derived from the use of surveillance cameras, for example. The use of modified images should be treated with even greater caution in case they prejudice the rights of those caught on camera.

The use of pixillation and other techniques would be acceptable however, for protecting the interests of those not caught up in the story.

Questions of accuracy have a great significance for those whose lives have been caught up in some special event which serves the public interest and therefore may legitimately be placed in the public domain. The research conducted among survivors, already referred to, shows that attention to detail was key in the acceptance by survivors of the use of images or stories.

"I would have made sure that all the facts were right . . . her age was right, the area we lived in was right, niggly things . . . we don't live in—that annoyed me. And the ages of my children were all wrong . . ."

8 September 1997

Letter from the Association of Chief Police Officers in Scotland

I refer to the consultation paper in connection with the above subject and would advise that this matter has now been considered by our Crime and Technical and Research Standing Committees. The Association would make the following comments and observations in relation to the questions posed:

1(a). What is the current and forecast future use of digital technology for image collection, storage and transmission?

Current usage of digital imaging is mainly confined to the Scottish Digital Prisoners Database held at the Scottish Criminal Records Office (SCRO) where there are 50,000 stored images. Over the next few years the number of stored images is expected to rise to approximately 400,000. Additionally three Forces either use or are introducing the use of digital cameras as part of their custody processing systems. Some Forces possess basic enhancement/manipulation software packages but there are no plans to use original or altered digital images for evidential purposes. It was felt that digital imaging currently occupies a niche area and is not expected to supersede analogue film in the short term.

1(b). What is the state of the art of image manipulation?

Computer software packages currently available for digital image photography afford the operator the ability to fully manipulate an image whether in analogue or digital format. Examples include the ageing of a person, the retouching of a post mortem portrait to create an acceptable image for release to the media, simply changing hairstyles or the creation of a facial image from a skull. As the software is not specifically produced for use in the criminal justice system, a comprehensive audit trail facility is not normally included. It is not known whether, if commissioned, a bespoke audit trail could be included to satisfy evidential requirements.

2. Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean they should be treated differently when used as evidence?

We agreed that it would be difficult to distinguish digital copies from the originals without the inclusion of an appropriate audit trail. However, by focusing on the principle of continuity of evidence, administrative and/or technological safeguards can, and must be, incorporated in enhancement procedures in order to provide the necessary security and authenticity for the data.

The SCRO software programme which maintains the Scottish Digital Prisoners Database has a number of safety factors built in, which preclude the manipulation of images outwith strict parameters. Any identifications made through this medium can be printed and used as productions. The SCRO imaging system is subject to the same standard of security as the criminal history system and a full audit trail is maintained for the latter. There exist already, therefore, procedures for safeguarding records within the SCRO, and these measures should provide a head start for establishing acceptable protection against tampering and manipulation of digital images.

Members have emphasised the need for highly trained operatives to control digital imaging systems and who, if necessary, could provide expert evidence in court to authenticate the images produced and explain the procedures used to generate the different copies.

3(a). *Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence?*

Whilst some members felt that they had insufficient knowledge to the detailed application of watermarking to images in order for them to comment on this matter, it was generally felt that the ability to create a means by which a first generation digital image could be identified would be an advantage in terms of its acceptability as evidence. Whether the application of watermarks alone to images would be sufficient to authenticate them for evidential purposes is not known and may be worthy of further research.

3(b). *What would be the preferred practical measure?*

Some members felt that the use of watermarks, in conjunction with a storage facility which cannot be altered, such as one based on a writable CD ROM, would provide the ability to "prove" an original image and show the various stages of enhancement/alteration it had undergone.

Other members advised that the preferred option would be a "fast fourier transaction" of the image which would be stored remote from the original. Any allegation of tampering could then be proven or disproven by taking a "fourier transform" of the image again, inverting it and thereafter adding it to the original "transform" in order to visibly detect any changes made.

4. *Under what circumstances and with what controls should modified or enhanced images be used as evidence?*

We are advised that no plans exist, within SCRO or elsewhere, for the storage of enhanced or modified images. However, it is possible that there may be a need to enhance or clarify images of poor quality, especially in relation to serious crimes. In these instances, whilst ensuring continuity of evidence, the processes of enhancement or clarification should be documented and open to examination.

It is believed that new European Directives due to be brought into force in 1998 may address at least part of this problem by declaring "a person shall not be convicted on video evidence alone". If incorporated into any proposed legislation, this would make it essential that corroborative evidence if submitted in support of any type of video/CCTV imagery produced as evidence in court.

5. *Do technologies which compress data or use error correction technology when transmitting it raise special problems?*

Some members were concerned that the very nature of technology which gathers information and breaks it down for transmission before reconfiguring it upon reception may not satisfy the Rules of Best Evidence and that this area must receive particular attention with a view to producing detailed guidelines. They felt that the integrity of the system must be maintained by way of an audit trail and evidence given by a specialist witness.

However, the members of the Technical and Research Standing Committee felt that although the compression of data provided a theoretical opportunity for loss of quality, it was not thought to be a major issue, particularly where verification protocols are incorporated into the transmission procedures.

It was noted that compression of data is an established technique; currently "Livescan" fingerprint images are compressed for use and ease of transference using ISDN telephone lines and, to date, no evidence has manifested itself to suggest that any alteration or image migration has occurred.

6. *Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?*

Surveillance cameras, continue to be an extremely powerful tool for intelligence gathering as well as in the prevention and detection of crime. Members did not perceive them to threaten civil liberties in any way when used practically and with common sense. There is, of course, a potential threat to civil liberties from the uncontrolled use of surveillance cameras, but members felt that the placement and use of police surveillance cameras is already strictly controlled as is the release of information from them. The levels of authority required for their installation, and the existing guidelines for their use by police forces, adequately maintains the strict control necessary.

In relation to the management of City Centre CCTV systems, members felt that their use should only be instigated following full and open discussion with a working group composed of members of the public, from the area concerned, who were broadly representative of the community. Codes of practice, operating guidelines and minutes of agreement should be composed, clearly stating the purpose of the system, camera control protocols, tape management procedures and criteria in relation to the release of information. Civil liberties issues are thereby addressed and such systems are controlled in the absence of legislation.

7. Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?

Members felt that the introduction of statutory controls on the placement and use of surveillance cameras by the police and the release of information from them was really a matter for Government which may, in the future, decide to introduce such legislation. Any legislation which is introduced should be no more or less restrictive than the existing guidelines which, members agreed, successfully govern the deployment of surveillance cameras and the handling of the information from them.

In relation to city centre CCTV systems, members agreed that, in the absence of statutory control, it is up to the industry, system owners and the police to ensure that camera systems sighted in public places are self-regulated and are operated in accordance with comprehensive codes of practice.

I trust that these comments will be of assistance.

R Cameron, Chief Constable, Hon Secretary

10 September 1997

Letter from The Law Society of Scotland

The Society has the following comments to make:

1. What is the current and forecast future use of digital technology for image collection, storage and transmission? What is its use by the courts and the legal profession? What is the state of the art of image manipulation?

It is likely that there will be increased use of digital technology in relation to such aspects as collection and storage of data and transmission between locations. Now there is a greater shift from paper and other forms of data storage to digital forms of storage collection and transmission, the safeguards in respect of digital technology require to be enhanced.

Digital technology could be used by the courts and the legal profession in relation to the presentation of evidence and the postulation of theories in a court context eg virtual reality presentations to enhance jury understanding of complex fact situations.

2. Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean they should be treated differently when used as evidence?

The ease of copying, manipulating and tampering with digital images does require a different treatment when they are used in evidence. There should be a clear audit trail and the necessity for some form of encryption in respect of the evidence should be considered.

3. Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence? What would be the preferred practical measure?

Special measures to authenticate digital images would increase the utility as evidence. The Society has no practical experience to offer.

4. Under what circumstances and with what controls should modified or enhanced images be used as evidence?

Modified or enhanced images could be used as evidence providing the nature of the modification and the nature of the enhancement are clearly stated prior to their use and an adequate comparison with the original is provided.

5. Do technologies which compress data or use error correction technology when transmitting it raise special problems?

No Comment.

6. Do surveillance cameras, particularly if used in conjunction with image tracking software, threaten civil liberties?

No comment.

7. *Should there be statutory controls on the placement and use of surveillance cameras and release of information from them?*

There should be statutory controls on the placement and use of surveillance cameras and the release of information from them.

8. *Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?*

Further advice for training should be provided to law enforcement officers and the courts on the technical limitations of this technology. Adequate guidance should also be provided by Government to law enforcement officers on the use of such technology.

9. *Is there the need for special measures to control the publication of modified images by the media?*

No comment.

I hope the foregoing is of assistance to you.

Michael P Clancy, Deputy Secretary, Law Reform

8 September 1997

Memorandum by the Chartered Institute of Arbitrators (Scottish Branch)

The potential problems relating to images used as evidence are, in my opinion, much further reaching and much more immediate than they might seem. Colour laser photocopiers commonly feature editing facilities. Tampering is therefore not a preserve of computer science. The immediate question relates to images but surely the problem is much wider. Virtually any document created is machine readable. If it is machine readable then it is machine editable. Letterheads are so easy to reproduce that they can play no part in establishing authenticity. That logically takes one to the third question of communications that are never committed to paper and always remain purely machine readable-e-mail.

I believe that the problem of authenticity might conveniently be considered alongside accuracy. The intended or unintended manipulation of images. I am not aware of any certain process by which authenticity or accuracy can be assured. A general purpose quality regime may assist but cannot assure. I believe it is necessary to go beyond the face of the problem. Why do people wish to use images as evidence? In most cases I believe the answer would be ease of retrieval. Images per se do not assist significantly. One of two other techniques are needed. The first is to tag an image to a database. The second to be able to search within the document itself. (Database tagging or optical character recognition.) The first is judgmental but it is no different to a manual retrieval system. Provided the image can be compared with an original as part of the audit process I see no way to further ensure that the image has not been manipulated. I do not believe water marks would help as they are only an image in themselves.

I believe the greater problem, both in terms of accuracy and tampering, lie in the province of optical character recognition. Manually reading every document and allocating it to a database leads to a very large element of cost in litigation or arbitration. If documents can be scanned and then converted into a machine readable and searchable format then, on the face of it, considerable savings can be made. Enhancement of the image is usual. The algorithms are complex and variable. After enhancing the OCR engine will commonly apply spelling, grammar and syntax algorithms to fill in unrecognised gaps. The judgement has now become machine intelligence and that cannot be tested. It is surely here where the greater dilemma lies.

SUMMARY

- Modern colour laser photocopiers make the problem more immediate and pass beyond computer scanning systems.
- We are not aware of any foolproof system preventing tampering.
- Tampering and inaccuracies lead to the same result.
- A good quality assurance system with traceability to the original documents is probably currently the best in our opinion.
- The increasing use of OCR technology should not be disregarded as it introduces the beginnings of machine intelligence and judgement.

D. Carrick

25 September 1997

Memorandum by Screen PLC

1. Screen plc is a public company listed on the London Stock Exchange Alternative Investment Market (AIM). The mission of the company is to be the UK's most respected provider of advanced products and services to the Security Industry and its customers. Through its Karline and Petards companies, Screen has installed CCTV command and control products in more than 30 major town and city systems run by local authorities and the police. It has also installed systems for security in a range of locations from HM Prisons to commercial and retail premises. In the majority of such schemes, the company's products act as a control point around which a variety of products and technologies from other manufacturers are integrated with those from Screen plc. The company has therefore a privileged vantage point from which to understand the technology developments and the needs of customers.

2. Digital handling of video signals is not new. In large CCTV systems, the video signal is already being converted between analogue and digital forms a number of times. A major reason for this is to avoid the degradation of the video picture which occurs in the handling and transmission of analogue signals, which is usually more severe than any degradation which might occur at each conversion from digital to analogue and vice versa. The modern CCTV camera is digital. For compatibility with earlier systems, it is conventional to convert the signal to analogue format before it leaves the camera. The signal, however, may then be converted to digital format for transmission over a fibre optic or other link between two locations and reconverted to analogue format at the receiving point. To record video signals efficiently (there obviously an important commercial imperative for this) a number of analogue signals may be converted to digital format, digitally compressed, and combined (multiplexed) before recording on a video tape recorder. They are then separated (demultiplexed) and reconverted to analogue format for later use or display on a television screen. The processes of analogue to digital conversion and its inverse are therefore already an integral and accepted part of the handling of video signals. Conversion to digital format at an early stage of the process (such as at the camera) contributes to the best fidelity of the final image.

3. With the major domestic market of multichannel home entertainment television, in which many television channels are compressed digitally into the frequencies previously used for a few analogue channels, high quality digital technology for video signals is rapidly becoming inexpensive. It will quickly displace analogue technology. The digital handling of all types of image in future is inevitable. Although semiconductor hardware is currently used for the processing, the next step is to carry out the digital videocompression in software which could be even less expensive and more easily updated. Such developments are likely to be commonplace by the end of this decade.

4. The ability to carry some 16 different digital video signals over the same communication link that previously carried just one analogue video signal of similar quality means that there is an overwhelming economic drive to use digital video signals over broadcast networks, videoconference links, or the links used in CCTV security systems. An important consequence of the use of digital videocompression is that the cost of transmitting video signals over long distances falls by at least an order of magnitude as compared to equivalent analogue signals. Together with the steadily downward movement in the costs of telecommunication circuit use, this makes the concept of interconnected and networked video security almost inevitable in the future.

5. The concept of analogue video signals being less immune than digital signals to manipulation or tampering is false. Analogue signals can be digitised, altered and reconverted to analogue signals. The television broadcast environment has led to the development of editing and special effects workstations (such as those produced by the world-leader Quantel, based in Newbury) which can carry out virtually any kind of manipulation of images in the digital environment. Such equipment will decrease steadily in price in the same way that personal computers have become more powerful and have decreased in price. With either analogue or digital video signals, a protective measure must be applied where the fidelity of the information is crucial. Techniques are now available for "watermarking" both analogue and digital signals to monitor if any changes have been made. Such "watermarking" would be the most practical technique for video signals used as evidence and the technique has already been demonstrated in the UK by Thorn EMI Central Research Laboratories, now an independent company, CRL.

6. Despite what has been achieved in enhancing video images from space, there could be dangers in enhanced images for legal purposes. The solution for the future is to achieve adequate quality in the source image for the required purpose. Digital compression assists in this by concentrating resolution in areas of detail. There is no reason why future CCTV cameras using digital compression should not provide broadcast television quality.

7. In all Screen plc products, a very high priority is attached to privacy and confidentiality. For example, the Screen Alarm Verification System uses video cameras to filter out false alarms, but signals from these cameras can only be addressed when the customer provides positive authorisation for this.

In our experience of large CCTV systems, very few complaints regarding privacy, or the lack thereof, have been received by our customers from the public. Electronic "censorship" is available in the form, for example, of certain privacy zones (certain areas within the camera field of view which are not viewable). Such facilities, with digital technology, can be enhanced as required by the customer.

More important is the quality of the operational procedures and the control exercised over viewing and recording. More thought needs to be given to the setting and monitoring of standards in this area.

8. Training in the use, implications and understanding of digital video technologies is important. A vital component of the installation work carried out by Screen plc is the training of those that will use the system.

Owen Williams (Chairman)

John Forrest (Director)

5 September 1997

Memorandum by AEA Technology plc

SUMMARY

1. As digital images are easy to copy, and it may be difficult to distinguish a copy or a doctored copy from the original, concern has been raised over their use as evidence. State of the art software from the UK will enable digital image files to be signed off at source, with a verifiable signature from a particular person. Any subsequent tampering (other than simply viewing) with any of the contents of the image file will result in immediate corruption of that copy of the file, and thus distinguishing it from a pure, un-retouched image. Signed images will also carry time and date stamps, for audit purposes. The underlying technology has been developed over several years, and the application of this technique to electronic documents files is running in pilot applications this Autumn 1997.

THE PRINCIPLES OF THE SYSTEM

2. The operation of the electronic authorisation system Authosign is simple because it follows the principles used for document and image management that are commonly used already. Thus, a document is prepared in the normal way, using Microsoft Word, Excel, etc. A digital image would be captured as a bitmap or some other electronic data file. All this is well established technology.

2.1 After the document is prepared, the authorising person's signature is captured, by a digitiser tablet, (a standard "off the shelf" piece of computer equipment; such devices have been around for 5-10 years.) It is verified automatically against the electronic records of the organisation and, if genuine, added electronically by the software to the document. (Such verification of a person's identity by their signature has been used by the Employment Service to check hundreds of thousands of signatures.) If it is not a genuine signature, or a bad specimen from that person, the signature is rejected. During the authorisation (which takes only a second or two), the check confirms not only that it is the signature from someone on the database, but can also check the person has the appropriate level of authority to sign off the document.

2.2 The system time and date stamps it to complete the audit trail. This formal authorisation is the final stage of document preparation, prior to issue, just as with a paper based system.

2.3 The authorisation "locks" the document, marking it "SIGNED". The document/image can then be transmitted electronically to another location, or stored on a disk.

2.4 When the document is read (by any member of staff) the signature can be reviewed to confirm it is a certified document/image.

2.5 Authosign

- Guarantees the integrity of a document or image.
- Gives security by verified authorisation of electronic documents/images.
- Provides an automatic audit trail.
- Retains a widely recognised means of confirming certification by a particular person.

3. In response to some of the specific questions the committee has posed;

3.1 "Question 2. Does the ease of copying, manipulating and tampering with digital images, and the consequent difficulties in maintaining an audit trail mean that they should be treated differently when used as evidence?"

I submit that in the same way that reports and prints of photographs can be signed and dated, the software we have available should enable this to happen with digital images, so if the images are locked with the Authosign technology, the evidence can be accepted in the same way as it is currently with paper based documents/images.

3.2 "Question 3. Would special measures to authenticate digital images (eg, watermarking) increase their utility as evidence? What would be the preferred practical measure?"

I submit that if the image source is known, and a certification of authenticity can be created through the use of Authosign software, with the confirmation coming from a known and responsible individual under controlled conditions, such special measures to authenticate digital images should enable them to be accepted as readily as more conventional images on paper.

3.3 Authosign has the advantages of being simple to use and not demanding lots of specialised equipment, so I suggest it is a very practical measure, which uses currently available technology.

4. You also asked; Have you considered if any changes are needed to the law to enable it (Authosign) to be used—eg, the companies act?

4.1 I do not know for certain. However, the Authosign approach is the nearest possible electronic equivalent to a signature on paper, if I understand correctly the analysis of Chris Reed in his book on Digital Information Law (Pub Queen Mary & Westfield College 1996), and thus there may not need to be any changes to the law to allow it to be used.

As Authosign:

- shows the agreement of the authoriser to the contents of the document;
- authenticates the signatory's identity;
- displays the signature visibly in written form;
- and attaches the signature to the electronic document,

then meeting these criteria, according to Chris Reed, should satisfy the Statute of Frauds 1677. I believe this is one of the most demanding if not the most demanding statutes governing the signing of documents. (Interestingly electronic digital signatures (RSA type) do not do so as they do not attach the written signature to the document.)

This evidence has been submitted on behalf of AEA Technology plc.

For further information contact or any questions arising from this evidence please contact: Mr Andy Lewcock, Department Manager, AEA Technology.

August 1997

Memorandum by Dr Stephen Castell, Computer and Systems Telecommunications Ltd

1. The future use of digital technology for image collection, storage and transmission will be all but "total" in the developed world within the next 10–20 years, possibly much sooner (this does not mean that paper will become redundant, nor photographic film—no, these media will actually probably grow in absolute terms, but rapidly become a tiny percentage by volume of the images captured, stored and transmitted as digits, on other re-recordable technologies and media). The convention of "take a hard copy, just in case", still very common, will wither once storage, communication and retrieval systems become (legally) reliable (or, first the rich, and then everyone else in the new "Global Non-Nation-State" decide they don't really care for or need "hardcopy", since it only assists taxmen, bureaucrats and other prying busybodies*). The rapid advances of digital imaging technologies, from digital cameras, to photocopiers, to the Internet, to PCs, to broadband digital telecommunications and television (wireless and wired), to multimedia PCs, "network PCs", cheap (ie "sub-£100") and powerful image capture, compression/decompression, manipulation, editing, sound/vision/graphics/data/text/navigation "hifi" mixing and playback SOFTWARE (alas, not from many, if any, British companies) are all combining to accelerate a (developed) world plunging headlong into a totally digital image future.

The use of digital technology by the courts and the legal profession—and, indeed the legislature and executive in many countries—is also rapidly advancing (though not, alas, very rapidly in Britain). For example, when I get back to the UK (from 17 November onwards), I will send you a copy of the Australian Financial Review article of 24.10.97 "World first: Victoria's laws in cyberspace": "the Victorian Government is in the final stages of moving the parliamentary process and all Victorian statutes into cyberspace". Malaysia and Singapore, too, have ambitious plans or actual projects afoot for becoming "electronic democracies(?)" and having "totally electronic courts and judgments". On a personal level, I have up to a dozen expert witness litigation matters afoot, all of which involve firms of instructing solicitors, as well as (teams of) my Associate Consultants. All but a handful of these people are on the Internet and I now regularly "run" my projects via email and "attached file" documents, from wherever I happen to be: it makes for a 24-hour business day, since "the network never sleeps", but it does mean I can keep things going anytime, from anywhere. Within a year or two I expect to be also sending voice and image communications, probably even video clips and real-time voice and vision presentations (eg via Internet digital videoconferencing via Internet telephony). (I could do it now, but the cost-benefit equation, and the tedium and quality, of the technology are not yet totally conducive). What is fascinating is that LOCATION becomes unimportant. Who really needs to know, or cares, where by brain is physically located anywhere in the world, as long as they can communicate with it?—and, as digital image technology advances, the quality of the communication approaches, or even surpasses the "real proximate thing" (I will always be able to look my best, or better than my best, on a—digitally enhanced—remote videoconference "meeting", and no-one has to buy me lunch, or I them, afterwards! Indeed, I could totally re-invent my physical image and eg give myself back a full head of hair!).

2. Yes, until totally legally reliable technologies are developed (and they won't ever be, with current commercial "von Neumann architecture" digital systems—see my CLSR etc papers and eg submissions to the Law Commission on the "ontological untrustedness of computers" which I have already provided to your

Sub-Committee), digital images **MUST** be treated differently when used as evidence. Not by some artificial and irrelevant “admissibility” approach, but by firm action being taken **NOW** to ensure that in future any legal examination (eg a criminal court trial) which involves reliance on computer-generated evidence must first order a report **BY AN EXPERT** into the likely reliability of that evidence. I know this will be an unpalatable thought, because your Sub-Committee will quickly spot the large cost implications—but the cost of **NOT** getting expert testimony will eventually be infinitely higher and be measured in far more dangerous citizen distrust and social breakdown (**BETTER STILL, AN INVESTMENT IN DEVELOPING A NEW LEGALLY-RELIABLE DIGITAL MACHINE ARCHITECTURE WILL BE THE CHEAPEST APPROACH IN THE LONG RUN**).

3. “Watermarking” and any other so-called “authentication” technique inherently relies on the same digital architectures as the systems or digital images they are intended to “authenticate”. There is no reliable practical measure. Every supposed “uncrackable” system is crackable, eventually. Given the opportunity, an expert can cast doubt on almost any digital evidence however supposedly “authenticated”. “If it’s digital, it is inherently modifiable without audit trail” and that is the basic and overwhelming truth of the matter, with current commercial digital architectures.

4. Always call for an independent expert’s report, first.

5. Compression or error correction does not raise special problems, just amplifies the basic one “no (human readable) audit trail” (as well as that of “communicating in code” . . .).

6. Of course civil liberties are threatened (it is already possible for papparazzi to dream up any photo they want, digitally, and print it in a newspaper; equally the police are already able to “prove” someone was at the scene of a crime by undetectably modifying a digital surveillance camera image). On the other hand, if no-one really knows where you are or who you are—“you are only the digital image you permit others to see or know”—the concept of “civil liberties” (for the privileged, but growing, few) perhaps becomes redundant anyway—“digital image technology liberties” replaces it.

7. Whether there are statutory controls or not will make no difference—the technology of micro-miniature digital surveillance cameras, transmitting their images to wherever you want on the face of the globe by low-power wireless communications over public mobile telephone networks, satphones, the Internet, etc is dramatically advancing. We are about to enter a world not of “Big Brother is watching you”, but “Millions of Private Little Brothers are watching you (and you them)”. Such controls would never be enforceable, even if one could sensibly define them and draw them up in the first place.

8. Yes, of course advice and training should be provided to law enforcement officers. (I am not sure the word “further” makes sense, however—is there much/any such training provided already?) Above all, they should be taught to recognise when an expert investigation and opinion is required (that is, “usually always”), and not, eg try and oppose it.

9. See my answers to 6 and 7. You can try, but it is not going to work. You might “control” existing newspapers (but the Princess Diana “sensible and restrained” aftermath is probably only going to be a short-term effect) and television, but these are rapidly becoming far less powerful in terms of being “the media”. The new media is the Internet, or whatever broadband “private and personal” superhighway follows it, plus recordable Digital Video Disks, 3-D computer “games” using real-time collected images of real locations and real people etc, etc—in the free world, the horse is already well out of the stable.

NB The problem of trying to control these things by statute will not improve whilst there are no technically competent people drafting the statutes. For example, the definition in the Criminal Justice Act intended to modify the Child Protection Act specifically to make mere possession of an “obscene image” of a child an offence, whatever form that image is in (having in mind eg “zipped” files, protected by a PIN, downloaded from paedophile Usenet Group sites on the Internet), defines “pseudo photograph” as “any computer data capable of being transformed into a photograph”. Unfortunately, that definition makes **ALL** computer data (eg this email!) a “pseudo photograph” of an “obscene image” of a child, since, by use of appropriately written software any “Data” is transformable into any “image” you want!!

Dr Stephen Castell

6 November 1997

**Memorandum submitted by Lord Brain, Member of the Council of the Royal Photographic Society and
Chairman of
The British Photographers Liaisons Committee**

**AN EXPLANATION OF THE DIFFERENCES AND SIMILARITIES IN
CHEMICAL AND DIGITAL IMAGING**

I use the words Chemical and Digital Imaging because a photograph is defined in the 1988 Copyright Act as:

“photograph” means a recording of light or other radiation on any medium on which an image is produced or from which an image may by any means be produced, and which is not a film.

LENS SYSTEM

This is common to both methods consisting of interchangeable or zoom lenses the aperture of which is usually controlled electronically, the zoom usually being controlled manually either directly or through an electronic link. The lens system forms a small image which is then recorded to form a photograph as defined above.

It may be worth noting that although "shutter speed" will affect the aperture to be used and the resultant image the results are similar in both processes.

PHOTOGRAPH RECORDING

(a) *Chemical imaging*

A "virtual" image is formed in an emulsion, usually silver based, supported on film, paper or glass. Different emulsions have different characteristics as to the amount of information that is retained as the virtual image. These can relate to such things as colour or black and white, daylight, artificial light, infra-red or ultra-violet, negative or positive viewing. The way they react to high or low levels of light. The size of the grain which affects the detail that can be seen on enlargement. Finally, contrast which affects how small differences can be recognised. The last three characteristics can be changed to some degree by the processing, (see below).

(b) *Digital imaging*

Here the image is formed digitally by a light sensitive surface and the digital information is transmitted to a storage system. This storage system can be a computer chip, a computer memory device or some form of magnetic device, tape or disc. The digital information can also be viewed instantly on a screen and fed into a computer system. As with a chemical system what is recorded for later retrieval depends on the software which may be likened to the film characteristics.

I would note here that if the initial digital storage system mentioned above is of a fully secure WORM type (Write One Read Many (times)) then the secure retention of the original image could be as good as the virtual image in the chemical process.

PROCESSING OR RETRIEVAL

(a) *Chemical*

In this process the emulsion is treated in a series of chemical processes to turn the "virtual" image into a "real" image and to stabilise it so that it becomes a WORM as described above. Whether this WORM is formed as a negative or positive is not important as they can be equally easily handled later. It can be said that it is possible that the positive process records colour accurately. However, the way a virtual image is processed can affect its colour balance, its graininess, its contrast and its speed, ie the way it has retained information at low or high levels of light.

(b) *Digital*

In this case the digitally retained image is processed electronically from the WORM so that a "real" image can be seen on a screen or fed to some other device. Just as in the chemical process, the way this is done can effect the characteristics of this image. The problem is that while the WORM should not be able to be changed, the processing can and may be changed but see below.

LATER OR FINAL USE

It needs to be recognised that it does not matter much whether the Master WORM is held in Chemical or Digital form as scanning devices allow the image information to transfer from one to the other with great ease. Nevertheless, I will explain how both systems work.

(a) *Chemical*

In this case light, in some form, is taken from either WORM image and recorded on a supported emulsion or other chemical mix which is then chemically processed to reveal a final image. This final image will depend on what has been taken from the WORM. Is it the whole or part of a frame, is it a complete series of images or has cutting taken place, how much enlargement has occurred, what has happened to the colour balance? These are editing or processing factors. Then one can turn to modifications, by which I mean altering the final image by adding or removing details. This can be done in the chemical process but takes longer, needs a very skillful operator and is usually detectable by eye.

(b) *Digital*

In this case the basic data is retrieved digitally either from the digital WORM or through a scanning device from the chemical WORM. Exactly the same changes can be made digitally to those listed above and they can be made much more quickly and the results are much more difficult to detect visually. However, provided data from the master WORM and the final image are available in similar digital form it is not difficult to produce electronically another image that highlights the changes between the two. The same process could be applied to two chemically formed images but the reliability of this comparison could depend on the quality of the scanner used.

3 November 1997

Supplementary Memorandum submitted by Lord Brain

A BASIC GUIDE TO DIGITAL IMAGERY

A glossary of terms will be found at the end of this document. Any word printed in italics will be found there.

The Oxford English Dictionary defines “photograph” as “picture taken by means of chemical action of light or other radiation on sensitive film”.

“Film” can be positive, negative, colour or monochrome. Whichever, traditional film is *analogue*. The image is created with a continuously varying tone. Computer technology has made it possible to store images *digitally*. These images are either created using a *digital* camera, in which case, there is no film and the image is stored on a computer chip, or they are scanned from *analogue* transparencies (also known as “slides”), negatives or prints and stored in a *digital* file. These can be viewed on a computer screen, printed, *manipulated* or used to create a duplicate transparency. A *digital* image does not have a continuous varying tone. It consists of thousands of square dots called *pixels*. A *pixel* is the smallest plottable point on a computer screen or imaging system and it consists of 24 *bits*—8 *bits* per colour used on a computer monitor (*RGB*).

An original, *analogue* photographic transparency is first generation as is an original, *analogue* negative. Whether colour or monochrome, a print made from this film is second generation. An *analogue* or a *digital* duplicate made from an original transparency is second generation. A reproduction from a second generation print or an *analogue* or a *digital* duplicate transparency is third generation. At every remove, there is some loss of quality.

Once an *analogue* image has been scanned and digitized, any number of identical *digital* second generation copies can be made but there will be loss of detail in these copies. The original transparency is scanned at high or low *resolution* depending upon the intended usage. High *resolution* means many more *pixels* per inch than low *resolution*. The *pixels* are far smaller and cannot be seen with the naked eye. Regardless of the size of the *pixel*, each one still consists of 24 *bits* and consequently, high *resolution* scans use a great deal of *disk* space. Where the final intention is reproduction on paper, the larger the size of the intended image, the higher the *resolution* required to ensure the *pixels* do not become visible. The image may also be scanned at 32 *bits* to match the four colour process used for printing (*CMYK*)—that is, 8 *bits* per colour. With low *resolution* scans, there are less *pixels* per inch and they quickly become apparent if the image is reproduced beyond the capabilities of the scan. The final printed image will indicate considerable loss of clarity. When the intended use is duplicate transparencies, the original must be scanned at high *resolution* to allow for reproduction at any size. A low *resolution* duplicate will not be of reproduction quality but will be sufficient for audio-visual use where quality is of less importance. Modern computer technology has made it possible to store large numbers of images *digitally*. These are usually scanned at low *resolution* and can be viewed as “thumb-nails” on a computer screen, enlarged for closer examination, down-loaded for use in layouts and despatched *digitally* within minutes, anywhere in the world. These low *resolution* images serve much the same purpose as a printed catalogue and are not of sufficient quality to be used for reproduction on paper at anything other than very small sizes.

No *digital* image will ever be as perfect as the original *analogue* version and above all, no *digital* image will have the integrity of an *analogue* original. *Digital manipulation* is often used to ‘enhance and “improve” photographs. Extraneous items, rubbish, blemishes or people can be removed without trace—or introduced. For this reason, *digital* images should not be trusted. A *digital* image has no integrity. It is virtually impossible to discover that an image has been *manipulated* if it is done with care. The technique is simple. Every *digital* image consists of *pixels*. A blue sky will be a mass of blue *pixels*. A cloud in the sky will be grey and white *pixels*. If all the grey and white *pixels* are deleted and the space filled with blue *pixels*, copied from the blue area around, the result will be a cloudless sky. Similarly, extraneous people, buildings and rubbish can be removed or added. Whole areas within the picture can be shifted around within the image and elements from different photographs can be introduced simply by copying the required area from one photograph and transferring it to another in exactly the same way as paragraphs of copy can be transferred from one document to another. *Manipulation* is done on screen and the area within the image to be *manipulated* is enlarged so that each individual *pixel* is apparent. Deleting one here and there is very simple.

A damaged transparency can be restored by inserting appropriately coloured *pixels* into the damaged area and a second generation duplicate of very high quality can be achieved, provided the *analogue* original is available for high *resolution* scanning. If all that is available is a low *resolution* scan, this cannot be used to make an adequate duplicate of the original. It is possible to lower the *resolution*, but not to raise it.

A file, whether high or low *resolution*, uses a great deal of available *disk* space and for this reason, files are usually *compressed*. The industry standard for *compression* is called JPEG (Joint Photographic Experts Group). *Compression* removes *pixels* throughout the entire image. Where there are identical *pixels* next to one another, *compression* removes one of them. When the file is *decompressed*, something similar comes back again but not necessarily what was there before. A system called "anti-aliasing" compares each *pixel* and multiplies it with an average *pixel*. This prevents the jagged, stepped edges that might otherwise occur due to the fact that *pixels* are square but tends to soften the final effect considerably. There are degrees of *compression*. Minimum *compression* removes very few *pixels* and when the file is *decompressed* it is unlikely the difference would be noticed. But maximum *compression* removes many more *pixels* and *decompression* can produce a final image which is nothing like as good as the original. The more a file is *compressed*, the less satisfactory will be the final result. However, since images use a great deal of memory, *compression* reduces the size of the file considerably.

Computer Technology has created a logical language of its own. Because everything is *digital*, this language is based upon *binary* mathematics. A *bit* is the smallest unit of computer information. A *byte* is a unit of computer memory which equals 8 *bits*. A *Kilobyte (Kb)* is 1,024 *bytes*, a *Megabyte (Mb)* is 1,024 *Kb*, *Gigabytes* and *Tetrabytes* follow, each achieved by multiplying the lesser figure by 1,024. 1,024 equals 2^{10} .

Where the reproduction of images is concerned, there is a mathematical rule of thumb for determining the size of a *digital* file. The size required in inches is multiplied by $dpi \times 2$ ($dpi = \text{dots per inch}$). What determines *dpi* is the intended quality and size of reproduction. The higher the figure, the better the final result. Thus for a reproduction at $12'' \times 10''$ for printing in a publication at 175 *dpi* for example, the formula is $175 \times 2 = 350$, $10'' \times 350 = 3,500$, $12'' \times 350 = 4,200$. $3,500 \times 4,200 = 14,700,000$ *pixels*. At 24 *bits* or 3 *bytes* per *pixel*, this equals 44,100,000 *bytes*. To turn this into *Mb*, the figure is divided by 1,024 twice. Thus, the result for a $12'' \times 10''$ reproduction is a file size of 42.06 *Mb*. For reasonable printing at $12'' \times 16''$ at 175 *dpi*, a file size of 67.79 *Mb* would be required. A $12'' \times 16''$ This is a fairly large reproduction. For newsprint, the file size would not need to be so substantial but for any publication requiring quality reproduction, this file size would be too small. Such printing would require a 32 *bit* scan and the files would be 33 per cent bigger.

However, for reproduction quality duplicate transparencies, the figures need to be multiplied by four which should produce reasonable results for normal use but not for the creation of photographic prints. Without a file of massive proportions, it is impossible to make a duplicate capable of creating a photographic print which will come anything near the quality of an *analogue* print from an original *analogue* transparency.

GLOSSARY OF TERMS

Analogue

A method of storing information by making proportional changes in a recording medium. Photographically this means a continuously varying tone.

Binary

A counting system based on the powers of 2. Two states are possible. "ON" = 1 and "OFF" = 0. Computers use the binary system because it is easier to get electrical circuits to retain "ON" and "OFF" states than the in-between values needed to represent the decimal system.

Bit

The smallest unit of computer information, based on the binary system.

Byte

A unit of computer memory composed of eight bits which also occurs in multiples

Kilobyte(Kb) = 1024 bytes (2^{10}), Megabyte(Mb) = 1024 Kb, Gigabyte(GB) = 1024 Mb, Tetrabyte(Tb) = 1024Bb.

CCD

Charge Coupled Device. A light sensitive chip that converts light into a digital value in scanners and digital cameras.

CD-ROM

Compact Disk Read Only Memory. A development of technology designed to store large volumes of text to other data, including photographs, which can be read but not altered.

CMYK

Cyan, Magenta, Yellow, Black. "K" means Key and equals Black. These are the four colours used in four colour printing.

Compression

The techniques by which large digital files, especially those including pictures which use a great deal of disk space, are made smaller without the loss of critical information. (see text).

DAT

Digital Audio Tape. DAT has survived as a name but the tape is now used for purposes other than audio.

Data

Information, however stored or recorded in a computer.

Decimal

Our normal counting system, based upon the power of 10, sometimes called Denary.

Digital

Any type of information using long sequences of numbers which can be understood by a computer. These numbers can be converted by the computer into prints, transparencies or colour separations for printing.

Disk

Never disc! The most common recording medium for storing data in a computer. A floppy disk is flexible and covered with metal oxides enclosed in a protective casing which fits into the "disk drive" slot in a computer. It is mobile and can be used in any computer. A hard disk contains one or more rigid magnetic disks in an enclosed case usually within the main body of the computer. Hard disks have a much higher storage capacity than floppy disks and often comprise the main part of a computer's memory.

Dpi

Dots per inch. Used as a measure of both scanner and printer performance. In general, the greater the number of dpi, the better the resolution of the image.

Film Recorder

A device which produces colour transparencies from a computer file.

Frame Grabber

A device for taking still pictures off video sources.

Hardware

The equipment comprising a computer system such as the Central Processing Unit(CPU), the monitor or screen, the disk drive, keyboard and printer.

Hexadecimal

Counting system using a base number 16, often used in computing.

ISDN

Integrated Services Digital Network. Advanced telephone lines designed for faster and clearer communication and necessary for images.

Manipulate

To change the appearance of an original picture using a computer.

Pixel

The smallest plottable point on a computer screen or imaging system. In the simplest monochrome system, such a point is described by a single byte or eight bits of computer memory and appears as either black or white on the screen. In a colour system, a single pixel requires more information to record its colour and intensity. The resolution of a digital image is expressed in pixels per inch. In general, the larger the number of pixels per inch, the better the detail shown.

RGB

Red, Green, Blue—the colours used in computer monitors and coloured photographic emulsions.

Resolution

A measure of the sharpness or detail recorded in an image. This can be expressed in different and confusing ways. Dots per inch derives from printing technology and pixels per inch from computer technology. The confusion is increased by the fact that in printing technology, dots are round and require a minimum of four colours, cyan, magenta, yellow and black (CMYK) and are subtractive whereas in computer technology, pixels are square, are based upon red, green and blue (RGB) and are additive. However, dots and pixels are interchangeable.

Scanner

A device for taking conventional graphics, text or photographs into a computer. The original image is scanned point to point by a laser beam, each point being assigned a digital value. A film scanner is used for scanning photographic transparencies and a flatbed scanner is for prints, artwork and copy.

Software

The digital instructions that make a computer perform specific functions. These are written by programmers in one of many computer languages which are usually incomprehensible to those who use the software.

WORM

Acronym for Write Once Read Many. A CD-ROM or optical disk which can be written once and read as often as required but which cannot be re-written.

WYSIWYG

Acronym for What You See Is What You Get. It means literally that. What you see on the screen is what you will succeed in printing—and no more.

Memorandum by the Faculty of Advocates

The Select Committee on Science and Technology have issued a Call for Evidence in relation to the future use of digital images within Court proceedings. The Call for Evidence focuses on the need for wise investment decisions to be made, presumably by potential litigants, practitioners and indeed the Courts themselves. However, a basic problem arises from the definition of what is encompassed by the expression “digital imaging”. Digital imaging is at present very much a part of every day business life with routine use of applications such as scanning of text and graphics, sophisticated photocopying using digital technology and, of course, use of digital cameras. The Call specifically relates to digital imaging but most of the comments made below could equally be applied to other forms of digital information storage. The Faculty’s Response follows the numbering of the questions set out in the Call of Evidence.

1. The Faculty is not aware of extensive use of such technology before the Scottish Courts although it is aware of an increased willingness amongst Scottish lawyers to consider using such technology for the storage and retrieval of large numbers of documents. Whilst increased use of such technology is likely, the Faculty is unable to forecast the extent of such an increase.

2. In principle, the Faculty considers that the case of copying and manipulating digital images would justify the introduction of special rules for dealing with digital images as evidence. A distinction must, however, be made between criminal and civil litigation, as different concerns arise. The higher evidential requirements under criminal law may render digital technology less problematic in that every document requires to be agreed, proved or meet certain statutory requirements regarding notice in order to be deemed to be proved. However, some aspects of the civil law of evidence do raise concerns with respect to new technology. While, in theory, there has always been a risk that documents may have been manipulated, digital imaging now makes the alteration of text documents and graphics to a high standard within the ability of any person with access to a personal computer. The ease in which documents may now be altered brings into sharp focus the already apparent deficiencies of rules of evidence such as Sections 5, 6 and 7 of the Civil Evidence (Scotland) Act 1988. The provisions of the Act do not reflect the Scottish Law Commission’s proposals regarding notice to be given to the party against whom a copy document is deemed to be proved. The adoption of the Scottish Law Commission’s proposals and the formulation of rules requiring notice would at least involve recognition of the possibility that the copy document has been altered or corrupted. Parties would then require to prove the copy relative to the original unless otherwise agreed. A perhaps incidental problem arising from the ease in which documents can be digitally canned and stored on CD-ROM is that in the course of litigation a party might be tempted to produce every conceivable document without giving much thought to their relevancy. This may lead to further overloading of the Court system and protraction of litigation.

3. The Faculty considers that special measures to authenticate digital images may be one solution to the problems identified in question 2 but given the lack of detailed contact with such technology, the Faculty does not feel qualified to comment on the various options.

4. There may be instances where modified or enhanced images would be valuable in the course of litigation. The Faculty considers that there should be rules to control the use of such evidence. Such rules could require both the modified and unmodified versions to be lodged in Court and in the absence of agreement between parties on the authenticity of the modified image, a requirement for proof of the modified image by expert evidence.

5. The Faculty considers that data compression or the use of error correction technology would be more likely to carry the risk of corruption rather than deliberate manipulation. Corrupt data may, however, be easier to detect than that which has been altered with the intention to deceive.

6. The Faculty considers that whilst, in theory, the use of surveillance cameras, may pose a threat to civil liberties, it is not convinced that the public interest has been adversely affected by such cameras. Such cameras have become an increasing feature within many Scottish cities which a resultant beneficial effect on the level of street crime. On balance, the Faculty considers that the public have generally benefitted from the presence of such cameras.

7. The Faculty accepts that there may be a case for some statutory control over the use which can be made of information from such cameras, especially by the media, although it is not convinced that controls are required on the placement of cameras.

8. The Faculty agrees that further training and advice is required to law enforcement officers and the Courts in relation to this technology.

9. The Faculty considers that the media have, on occasions, acted unfairly by using modified images and it would support special measures which would either restrict the use of such images or would clearly indicate when images have been modified.

Edinburgh

January 1998

Memorandum by Crown Prosecution Service

BACKGROUND

1. Video and photographic evidence is used in criminal proceedings with increasing frequency. Such evidence can arise from:

- Surveillance cameras in city centres. The widespread use of security surveillance cameras in city centres has resulted in video evidence being used on a very frequent basis, particularly when prosecuting public order offences, criminal damage offences and assaults.
- Surveillance cameras in shops, business premises and domestic homes. Video evidence is commonly used in prosecuting theft and burglary offences.
- Covert police surveillance operations.
- Video cameras placed in police vehicles. These are used in enforcement of motoring offences. They are also used in recording scenes of crimes and serious road traffic accidents.
- Video evidence played in court as a child's evidence in chief in certain child abuse cases.
- Fixed roadside cameras used for traffic enforcement.
- Video film identification under Police and Criminal Evidence Act Codes of Practice Code D.
- Photo-fit pictures to assist in identification of a suspect.
- Cameras placed in custody suites and interview rooms in police stations.
- Photographic evidence (still frame) obtained by police photographers. Such evidence is used frequently in assault cases to show injuries. It is also used in offences against property to illustrate the property involved or the damage done to property. It may also be used to show the location and locality of an offence.

2. This list, although not exhaustive, illustrates that video and photographic technology is already frequently used as evidence in criminal trials. The developments in digital imagery and the pace of these developments mean that the impact of this new technology in criminal trials is likely to be considerable.

QUESTION 2

Does the ease of copying, manipulation and tampering with digital images, and the consequent difficulties in maintaining an audit trail, mean they should be treated differently when used as evidence?

3. When a video recording of an accident or a photograph is to be used in evidence, its relevance must be established by the testimony of someone with personal knowledge of the circumstances in which it was taken or made. In the case of a video recording, its provenance, authenticity and integrity must be proved, and the party relying on the recording must be able to establish an audit trail covering the tape from the time of recording to its appearance in court. Storage in a tamperproof environment is important. Criminal lawyers are aware of and used to ensuring that the relevant photograph or video meets these requirements. These requirements have all been developed by the common law.

4. There have been no cases, thus far, which set out any specific requirements to be followed in respect of digital imagery. Although we know of no cases on the point, we believe that the ease with which digital images can be altered may lead to assertions that the image before the court has been tampered with and should not be relied on. As with basic video technology, we should be able to rebut such assertions if we can show a proper audit trail and that the disk on which the image is stored has been kept in a tamperproof environment.

5. To a large extent, before the introduction of digital technology, the integrity of the evidence was rarely challenged as there was general public awareness that videotapes could not be easily tampered with and altered. If the prosecution were put to strict proof on the audit trail and the integrity of a video tape in all cases, the resource implications would be considerable. One of the consequences of the widespread use of digital equipment in the home environment is that the ease with which such images can be altered is already widely known, so we do expect challenges on this point once digital images are used in court. Our ability to rebut a claim that an image has been tampered with will depend on how it was stored and the extent to which we can exclude external interference. To do this in a detailed way in every case where a digital image is relied

on could be very resource intensive. Unless we are able to do this, however, there may be a general doubt about the evidence and we could lose the case.

6. It may be appropriate to draw a distinction between digital images used by the police and those used by other organisations and individuals. Awareness of evidential requirements enables the police to include data protection/encryption requirements to a very high standard in specifications for digital equipment. The requirement to capture an image and secure it on a CD-ROM WORM drive at the earliest possible point, in a controlled police environment, ensures a high degree of security of the image.

7. Users other than the police do not always have the expertise to ensure a tamperproof audit trail. Their equipment may be of a lower specification and the image may have been recorded onto a disk or hard drive which could be overwritten. There may be a particular difficulty when relying on video evidence from surveillance cameras in CCTV systems. Such evidence is frequently used to identify offenders. The law does not make any real distinction between an individual who sees an incident on a monitor and an individual who views an incident at first hand, but if this were a digital image it could be suggested that the image shown to the witness was not a true representation of the incident.

8. It will be necessary, therefore, in rebutting these assertions, for any system to have within it some form of data protection/encryption operating. If the image is captured and burnt onto CD-ROM WORM drive at the earliest point, this would seem to overcome the difficulty. It would also be helpful if additional information such as the time and date when the camera commenced recording of the image and the time and date when the digitised image is captured and burnt onto a CD-ROM WORM drive were recorded on the image.

9. As with video tapes, the user of the equipment will also have to ensure that records are maintained of many other details of the system and its operation, for example it would be necessary for records to show:

- who was in control of the equipment at the time of the relevant incident;
- how the image is identified;
- how the image is stored;
- any instances when the stored image is retrieved/restored; and
- who was in charge of the equipment at the time of any event involving the image.

10. The records required to establish the integrity of the evidence will, in most circumstances, be capable of being included in the specification of any system to be used. They will need to be subject to the same level of security as the image itself.

11. We do have an area of concern so far as defence evidence is concerned. The ability to construct an alibi that is convincing has become cheaply and widely available by using home video equipment to manipulate an image.

12. Similarly, digital technology will enable false evidence purporting to show police acts of corruption to be constructed very easily. It would be easy to undermine the credibility of prosecution witnesses by constructed evidence and thus damage the prosecution process.

13. It would seem equitable to require a similar level of data protection on the part of the defence as required by the prosecution to meet these dangers. It may be argued that it is unrealistic to require that sophistication of data protection in the majority of cases where the defence were seeking to rely on a digital image. However, whilst the prosecution must establish a case beyond reasonable doubt, the defence need only create a doubt in the mind of the jury to secure an acquittal. We would be concerned if the defence did not have to establish a secure audit trail and the integrity of the image to a similarly high standard, as a digital image concocted to support a defence case could be used to secure a wrongful acquittal.

QUESTION 3

Would special measures to authenticate digital images, eg watermarking, increase their utility as evidence? What would be the preferred practical measure?

14. This is principally a technical question although it does have evidential implications. Any system which authenticated an image would assist in enabling the integrity of the image. A watermark could also assist in establishing ownership of the image. A watermark would have to be secured in some way that would confirm its nature and it would also be necessary to show who placed the watermark.

QUESTION 4

Under what circumstances and with what controls should modified or enhanced images be used as evidence?

15. Enhanced images, that is images where an improved image is achieved using technology to show all the detail that the image contained, do have a role in enabling a case to be presented in its best form. However, as with all evidence, any process which has been used must be explained in evidence and continuity with the original image established in a way that satisfies the court that the evidence is safe to rely on.

16. Modified images have undergone some process of change. That change may be required to show some aspect of the evidence in a particular way. However the fact and purpose of the modification would have to be explained. A court would undoubtedly be concerned that the effect of the modification was to undermine the integrity of the image.

QUESTION 5

Do technologies which compress data or use error correction technology when transmitting it raise special problems?

17. Compression of an image for storage purposes will not necessarily alter the image. As a process, it should be explained in the statement producing the digital image to the court, but the fact of compression should not in itself create a difficulty in relying on the evidence. Error correction technology will alter the image. This could affect the admissibility, although that would not invariably be the case. The use of error correction technology and its effect on the image would have to be explained to the court. The view the court took on its admissibility would depend on the extent of the interference and its purpose.

QUESTION 8

Should further advice or training be provided to law enforcement officers and the courts on the technical limitations of this technology?

18. We think it would be helpful for there to be an explanatory leaflet produced for lawyers and courts explaining the technology in a clear and straightforward way. We have become aware of the need for such documents when dealing with DNA evidence. DNA profiling is a complex scientific procedure and is difficult for the non scientist to understand. We have been involved in working with the Forensic Science Service to produce an explanatory leaflet for lawyers on DNA evidence which will be published shortly. This should assist lawyers and the judiciary in understanding some of the complexities. A similar leaflet on digital images for the judiciary, lawyers and magistrates could be useful in ensuring the technology is understood and court time is not spent simply on explaining the technology.

Jennifer Terry (Mrs), Team Leader, Casework Services Division, Crown Prosecution Service

14 November 1997

Letter from Professor Vicki Bruce, Professor of Psychology, Univeristy of Stirling

You ask about three issues which I will take in turn:

1. What technology can and cannot do, compared to what humans can and cannot do.

I will confine myself to the recognition of faces. When humans recognise faces they need to be able to match images across transformations of pose (head angle), expression, lighting and sometimes changes in weight, hairstyle and age. Human recognition of highly familiar faces (family, friends, celebrities) is pretty robust across such changes, but highly familiar faces have been stored in memory from a huge variety of different poses, expressions etc. Human recognition of relatively unfamiliar faces is poor, and legal history is full of cases of mistaken identity which arise from the fallibility of human face recognition (eg, see report by Lord Devlin's Committee, 1976).

Now that the faces of criminals may be captured on CCTV there is a temptation to assume that problems of human recognition disappear. It seems reasonable that, when the burden of remembering a face is removed, human perception should be able to judge whether a CCTV image is, or not, that of a suspect. Unfortunately, human vision has difficulties even in these circumstances, since two different images of the same person may still vary in lighting, pose and expression and such variations, even if very slight in terms of angle or facial gesture, make it difficult to tell if two images are of the same person or of two different people who look similar. In recent, not yet published, data in our laboratory we have found that volunteers asked to match a target image (taken from good quality video footage) against a line-up showing faces of ten people (rated as similar in appearance to the target person) make wrong choices in 20 per cent of these line-ups, even though the face images all showed the same, frontal viewpoint, and the volunteers were under no particular time pressure in these experiments. These data agree with a recent paper published by Richard Kemp and associates at the University of Westminster, who found a very high error rate when testing how well cashiers could verify identities of customers who had photographic identity cards.

In our own ongoing project we are aiming to compare human performance at matching images of this kind with the performance of certain computer systems. Our research to date has shown that the computer systems also fail in the circumstances described. This is because the image features used to match from a CCTV image to some other image format (eg high quality mugshots) can be very different, due to some differences in lighting and colour or contrast, as well as subtle variations in head angle and expression.

To the best of my knowledge, there are no existing computer systems for recognising faces which can deal successfully with these kinds of variations. Systems which report good performance at face recognition rarely deal with the range of variations present by images in daily life. Several systems are available which can deal with the problem of face verification, where the task may be to verify that the person whose face is presented matches their own identity stored on file, but this is a rather easier problem than the one of assessing which of a set of identities a particular face image matches.

2. What you see as the future if face recognition (its potential and possible applications).

In terms of recognition of identity from face images, many commercial businesses are now focussing on the identification of images of the human iris, where problems of false identification are much less likely to arise. However, typical CCTV images are unlikely to show images of the iris in sufficient detail to be useful. There is likely to be more potential by combining recognition of face images with other information, such as the voice (if available), movement patterns, height, weight and so forth. This is the way that the human brain usually identifies people—by weighing up evidence from a number of sources. The danger is that an image of the face is seen as being the pre-eminent source of information. It is probably the most important source, but the error rate needs to be reduced by combining with other information. Another source of development from the CCTV situation would be the use of multiple views taken from a video image which could be tested against multiple views held on file. There is a tendency to focus on “canonical” mugshots showing a small number of views, but there is no reason why mugshots should not show multiple images, which might help in the identification process. Improvements in the quality of CCTV images will also be useful in rendering the process of identification from this medium less error-prone. A final point here is that CCTV images may provide much less ambiguous evidence where the person shown is familiar to a witness. We are currently working on projects which illustrate how easily identity can be established from poor quality moving images of highly unfamiliar people. The usefulness of CCTV footage to prompt recognition of people on programmes such as *Crimewatch* should not be underestimated. What is not clear at present is whether such identification may be biased if someone is familiar with someone who merely resembles the person caught on camera. We are currently exploring this issue.

3. Whether the use of face recognition software, in your view, could raise civil liberty issues.

I don't personally see why software used to try to identify images of faces should cause any more civil liberties issues than using the human observer to scan the same images (by viewing the CCTV evidence) or using software to identify other things such as car registrations. The civil liberties issues seem to me to be overshadowed by the potential abuse of software which cannot do the job claimed of it. There are also many difficulties surrounding the enhancement of low-quality images, particularly where image-enhancement relies on some knowledge of the likely subject of the image.

I hope these brief comments may be of use. Please let me know if you want more detail.

13 November 1997

Memorandum by Niels J Bjergstrom, Managing Editor, Information Security Bulletin

These are very large and important questions. I can only present technical comments because I have no juridical education. I have worked with computers since 1964 and in Information Security since 1987. I am currently the editor of Information Security Bulletin.

As far as I can see, a fundamental problem to information security is the generation and attachment of a “digital identity” to an individual. Technically it would be possible to install such an identity into every newborn by operation, but such a process obviously raises currently insurmountable ethical problems. Nevertheless, I expect to see attempts in this direction within the next ten years, albeit not necessarily in this part of the world.

Such a method would by and large link digital creations and transactions irrefutably to individuals, and any and all changes to a digital representation would be possible to trace back to their originator.

While this technique is not yet in use we attempt to create digital identities by means of digital certificates issued by Certification Authorities, and rely on these to correctly identify an applicant and the connection between the individual and his or her digital certificate. Thus, the certificate is a digital representation of the individual. This authentication tool is not yet in widespread use and most systems that create what will in this connection ultimately be regarded as potential evidence, do not yet implement such techniques. For commercial reasons, however, it is beyond doubt that better authentication methods will be developed and broadly implemented. Thus, I expect to see the capability to irrefutably link an individual to any digital creation as something which will improve over the next few years.

These are general remarks. Methods such as digital watermarking are worthless unless they can be traced back to the originator of the watermarked document or image, but progress is being made with regard to authentication. I expect that more and more machines and processes (eg digital cameras and image manipulation programs) will require authentication in the future and incorporate this information inseparably into digital creations.

This brings us to the next tier in the chain of evidence: Forensic methods.

Whereas it is in principle possible to manipulate any digital representation as one might wish there are some practical problems that can be used by computer forensic experts to discover at least if an image has been altered after its original rendition, and in some cases also where in the image changes have been carried out. The methods in use are based on statistical sampling of adjacent areas of the image to see if there are colour or other gradients which are not consistent with the average information content of the image. I am sure that eg Mr Jim Bates of Computer Forensics Ltd will be able to furnish more qualified information regarding this subject.

Your item no 2: An important difference between digitally manipulated images and forged imaged produced by different methods is that it is possible to produce digital images of a quality requiring serious forensic examination to determine whether changes have been made. Until automatic methods to perform this have been designed, such examinations are cumbersome and very expensive. A leading computer forensics expert, Ed Wilding, writes in an article in the December issue of Information Security Bulletin, that "I would venture that forensic technology is now lagging behind 'state of the art' developments in home and business computer use." A serious remark by a man of his calibre!

In conclusion, digital evidence should be treated as taught at Bramshill and other places while in the care of authorities or forensic experts, and it should be DIGITALLY EXAMINED to discover if and how it may have been manipulated if presented as evidence.

Your item no 3: Cryptographic techniques embedded into images will irreputably prove if an image has been altered after a "digital watermark" was "embossed". It will also normally authenticate the producer of the image. It is important to note that including a digital watermark changes the image itself, so forensic experts or authorities cannot install a "digital watermark" without altering the evidence. However, this is not necessary either, because a one-way hash across an image combined with a good audit trail can be used to prove that no tampering has taken place. So, best practice would be to encourage producers of images to include "digital watermarks", and for examiners and gatherers of evidence to always take hashes or checksums of the files and store these separately in sealed evidence bags.

Your item no 5: I can't see error correction causing problems, because error correction only takes place when the error can in fact be corrected, ie the original image re-created. Error correction is normally applied to digital information such as programs, in which a single bit error can cause the program to fail. For this reason it is in fact correction, not approximation.

With regard to compression, particularly image compression, two radically different techniques are used. One technique (eg Zip-files) uses a type of compression, which only removes REDUNDANCY, not information, ie you can recreate EXACTLY the same image from the compressed version. Other techniques primarily designed to facilitate image transmission by reducing the amount of data contained in an image do result in information being lost, ie the original image can not be re-created exactly. This image compression may actually take place already when an image is captured, eg by an electronic camera.

The remaining items are of a political nature and thus outside the scope of my expertise.

14 November 1997

Letter from Office of Public Service Central IT Unit

At the moment there is no published guidance for Government departments on data matching. Under the Benefits Fraud Act, the Department of Social Security is preparing a data matching Code of Practice which is expected early in the new year. CITU will continue to monitor the position and identify the need to develop any further Codes of Practice.

Colin Muid

2 December 1997

Memorandum from Dr Nigel D. Haig, DERA, Fort Halstead, Sevenoaks, Kent TN14 7BP, on Automatic Face Recognition (December 1997)

Face recognition seems so intrinsically easy that it is difficult to accept that it is one of the most complex operations that a human being can be asked to undertake. Just considering the UK alone, for instance, we are each able to identify one single familiar face out of 60 million, given good lighting and a close view.

On the other hand, if we do not know how we recognise people, how can we program a computer to do it? Basically, most available techniques are very simple bottom-up methods that rely on the designer/programmer's intuition and experience. Currently this has proved to be inadequate, since no face recognition system has been shown to be any better than the others, in practical situations, and none of them is consistently better than humans. For example, humans find it easy to recognise a single face in a large crowd, yet computers still have difficulty in deciding which part of an image contains a face, without even getting as far as recognising it!

Times are beginning to change, however, and some work is now being actively pursued by various teams around the world along the general lines of the human visual/recognition system. Amongst others, this author is building an automatic recognition system that is firmly based upon the human prototype, with the research being funded by the Ministry of Defence, for application to vehicle recognition and face recognition. The assumption that lies behind this technique is that the human eye/brain recognises supremely well, so why not copy it?

This so-called top-down approach relies on mimicking the human visual system as closely as possible, using a TV camera and computer. Then certain types of self-organising Neural Networks are mounted on the back of the vision model. After a period of training the nets on typical imagery, they are made to “learn” the micro-features that go to make up a typical image. Then, whenever the Networks are shown a new image, such as a face, they are able to encode the face in a group of the “learned” micro-features that is characteristic of that one specific face. By comparing that particular grouping of micro-features with the similar record stored in long-term memory, identification should follow. There is good evidence that this is the way that humans do it, and it does seem a promising way ahead.

However, for the present, there seem to be no well-developed and reliable face recognition systems on the market, except for applications that are very tightly controlled (eg very powerful lighting, accurately positioned head, precisely specified range to the camera, and so on). This particular technology is beginning to evolve into specific and well-controlled applications, but it must be said that it is not yet mature.

Dr Nigel Haig is a Consultant Scientist on Vision and Optical systems with the Defence Evaluation and Research Agency, part of the Ministry of Defence. Dr Haig works on vision-related matters and electro-optic system design and development for defence applications.

December 1997

Memorandum by the General Council of the Bar

1. Digital images as evidence can be of different forms—the photocopy-like image of some text (ie static, inanimate), or the video-camera recording (which may involve movement) or purely electronic record, the use of digital media for ease of storage (rather than for replacing the original). Thus a distinction can be drawn where the evidence is created in digital form and when it is a digitised version of other materials (whether or not such original material exists). In some circumstances material sought to be relied upon may be a hybrid version, perhaps where original digital material is copied onto another item of media into a digital library of evidence.

2. From the Bar’s viewpoint there is a perceptible movement towards the use of digital image technology for use in more and more cases. The use of scanned images in courts has found favour in recent times. The ability to retrieve images rapidly on screen using computer technology saves time by avoiding handling files continuously, often for single pieces of paper. The use of CD-ROM for dealing with discovery materials is especially useful, and the ever increasing accessibility of the technology and the development of applications for lawyers, and litigators in particular, means this is likely to continue. Equipment costs, particularly scanners and image software, have fallen drastically in recent years. The ability to store many images on durable CD-ROM that are “write once” only has lent itself to the belief that the images are secure. The judiciary’s increasingly warm embrace of IT, particularly when used to make large cases manageable, seems likely to encourage further use. The attractions of potential cost and time savings has not gone unnoticed. The arrival of firms specialising in creating CD-ROM collections of evidence and offering to operate retrieval systems in the courtroom indicates the anticipated level of demand for such services.

3. At present the adoption of digital libraries of the evidence requires the original to be on hand in case of dispute—unless the parties agree otherwise, and so does not represent a replacement to the originals. In such circumstances whenever there is a dispute over an item of evidence the original can be reviewed and the conventional rules of evidence applied.

4. The BSI has issued codes of practice addressing the issues of legal admissibility of information stored on electronic document management systems (PD 0008) and also addressing the issues raised about information security management (BS 7799). These practical guidelines are relatively recent and take account of the Civil Evidence Act 1995. However, testing the extent to which users of such systems ensure that the codes are complied with is likely to be an area of practical difficulty. A more fundamental issue is their remit—being only to material stored on “write once, read many” (WORM) storage systems, such as CD-ROM. Where companies use archiving systems that are perhaps based on magnetic or magneto-optical media, the fundamental assumptions relating to the inability to alter material will be inapplicable.

5. Clearly, whenever information is manipulated there is the opportunity for corruption in the sense of loss of integrity. Any process that alters the data (evidence) whether to secure its integrity (by applying an algorithm to the data) or to “wrap” it in a secure form may lose the “original” status of the evidence.

6. CD-ROM may have a false appearance of security. The costs of equipment for copying and creating CD-ROM discs is falling rapidly—they are now widely available for about £270. The software for taking the contents of one CD and copying it is a standard inclusion with such devices. The software for amending the contents is almost equally widely available. As the media costs are now comparatively small (about £7 or less),

it is easy to conceive of tampering by means of reading and altering before re-recording to a fresh disc. The advent of the use of "cheap" rewritable CD technology will revert its consideration back to the same status as any other medium.

7. Thus some of the issues for consideration of CD-ROM materials as being primary evidence will be similar to those for other digitally based material, including those for video tapes etc. The need for a clear distinction between the information stored on the media and the computer system that is being used to access the media should be recognised. Clearly the evidence is on the item of media not the computer or application running. Previously legislation has centred round the computer that created the record, rather than the integrity of the record itself. The need for guidance on the interpreting of records created digitally, and/or automatically should be clear. The problem of formulating a practical approach to assessing the integrity of a wide range of records without incurring large costs is, unfortunately, equally clear.

8. The difficulty in detecting digitally altered material calls for caution when applying any presumptions to the admission of such evidence. The historical measures surrounding computer evidence viz, appearing to operate normally and being used for purposes which they normally were used, are less appropriate in current circumstances than when first introduced. The presumption of admissibility brought about by a certificate, which can be mass-produced, does nothing to improve the quality of the evidence itself. The inclusion of a requirement for a suitably knowledgeable person to provide some account of the handling and origin (where appropriate, and to what level of detail are issues in themselves) to accompany such a certificate would increase the value of such a certificate.

9. The "passport" type recording of operations involving digital media may assist, however it is unlikely that anyone tampering with material is likely to record the fact that they handled it. The use of devices which can record independently the work that they have done on items of media—like the transaction log on fax machines—may be one possibility, but is likely to require new equipment, and unlikely to be universally adopted, unless given statutory force.

10. The use of digital watermarks may be an attractive possibility, however the use of such technology would require expert evidence to assess the veracity of the authenticity or other attributes claimed. There would also need to be some measures to establish that the watermark was applied when it was claimed to be and that the simple expedients of change time-clocks and other measures could not "recreate" the watermark. If successive watermarks could be applied the history of a piece of evidence could be incorporated into it. Matters such as weight to be attributed to the watermark(s) will need to be established in the usual way as their introduction and reliability are shown.

11. The use of image enhancement technology, especially in criminal cases naturally calls for the balancing of sufficient explanatory information being provided with an understandable level of information which will not confuse. A detailed account of how the enhancement is achieved may be counter-productive, although the need for proof that the process can be relied upon is clear. The admissibility of the results of such processes as evidence is clearly a matter for the judge on a case by case basis; guidelines may assist, however a court appointed expert could also be a suitable means of avoiding confronting judges with difficult technical issues. The impact of the revised approach to civil justice may bring about some opportunity to implement this.

12. The widespread use of video surveillance, especially by police and other bodies associated with public events, coupled with the technology to match such images across different collections of data does raise issues over the protection of privacy. The view of the Data Protection Registrar over the merging practices of data processing and data matching of such information should be ascertained. The justification of such systems that have the ability to track individuals is questionable for all but the police and security services.

13. The use of compression technology which retains digital signatures within the compressed format and the integrity of the compressed image itself offers the opportunity for tracking items of evidence. The need to prove the signature can be addressed as a matter of evidence in the normal way of proving each item. A careful log of the actions of people when creating digital archives in accordance with the standards developed will also assist to create evidential weight. Alternatively, if the user or operator of equipment's identity is incorporated into the digital signature of the archive or other digital image which is operated upon then this will also enhance the audit trail.

John Horne

Secretary, Bar Services & IT Committee

ISBN 0-10-477798-2

9 780104 777985



Published by The Stationery Office Limited
and available from:

The Publications Centre

(Mail, telephone and fax orders only)
PO Box 276, London SW8 5DT
General enquiries *Lo-call* 0345 023474
Telephone orders *Lo-call* 0345 585463
Fax orders 0171 873 8200

The Stationery Office Bookshops

59-60 Holborn Viaduct, London EC1A 2FD
(Temporary location until mid-1998)
Fax 0171 831 1326
68-69 Bull Street, Birmingham B4 6AD
0121 236 9696 Fax 0121 236 9699
33 Wine Street, Bristol BS1 2BQ
0117 9264306 Fax 0117 9294515
9-21 Princess Street, Manchester M60 8AS
0161 834 7201 Fax 0161 833 0634
16 Arthur Street, Belfast BT1 4GD
01232 238451 Fax 01232 235401
The Stationery Office Oriel Bookshop
The Friary, Cardiff CF1 4AA
01222 395548 Fax 01222 384347
71 Lothian Road, Edinburgh EH3 9AZ
(counter service only)

In addition customers in Scotland may mail,
telephone or fax their orders to:
Scottish Publication Sales,
South Gyle Crescent, Edinburgh EH12 9EB
0131 479 3141 Fax 0131 479 3142

The Parliamentary Bookshop

12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders 0171 219 3890
General enquiries 0171 219 3890
Fax orders 0171 219 3866

Accredited Agents
(see Yellow Pages)

and through good booksellers

©Parliamentary copyright House of Lords 1998
Applications for reproduction should be made to HMSO

ISBN 0 10 477798 2